A R Q
22
SPRING 2000

THE JOURNAL OF THE DEFENSE ACQUISITION UNIVERSITY

ACQUISITION Review QUARTERLY

VOL. 7 NO. 2

The ***Acquisition Review Quarterly*** is published quarterly for the Defense Acquisition University by the Defense Systems Management College Press, 9820 Belvoir Road, Suite 3, Fort Belvoir, VA 22060-5565. Periodicals Postage Paid at Fort Belvoir, VA and at additional mailing offices. Postmaster send changes of address to: Editor, ***Acquisition Review Quarterly***, Defense Systems Management College Press, 9820 Belvoir Road, Suite 3, Fort Belvoir, VA 22060-5565. For free copies, submit written requests to the above address. Articles represent the views of the authors and do not necessarily reflect the opinion of the Defense Acquisition University or the Department of Defense. ISSN 1087-3112.

The ***ARQ*** is available electronically on the DSMC Home Page at **http://www.dsmc.dsm.mil**

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	Spring 2000	

4. TITLE AND SUBTITLE
Acquisition Review Quarterly (ARQ)
Vol 7, No. 2

5. FUNDING NUMBERS

6. AUTHOR(S)
Numerous Authors

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Defense Systems Management College
Attn: DSMC Press
9820 Belvoir Road Ste 3
Fort Belvoir, VA 22060-5565

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Defense Acquisition University
2001 N Beauregard Street
Alexandria, VA 22311

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Distribution Unlimited

12b. DISTRIBUTION CODE

13. ABSTRACT *(Maximum 200 words)*

The primary goal of the Acquisition Review Quarterly (ARQ) is to provide practicing acquisition professionals with relevant management tools and information based on recent advances in policy, management theory, and research. ARQ addresses the needs of professionals across the full spectrum of defense acquisition, and is intended to serve as a mechanism for fostering and disseminating scholarly research on acquisition issues, for exchanging opinions, for communicating policy decisions, and for maintaining a high level awareness regarding acquisition management philosophies.

14. SUBJECT TERMS
Cyber Warfare; Enterprise Architecture; DoD Acquisition; COTR Expert System Aid; Downsizing; Acquisition Force Structure

15. NUMBER OF PAGES

16. PRICE CODE

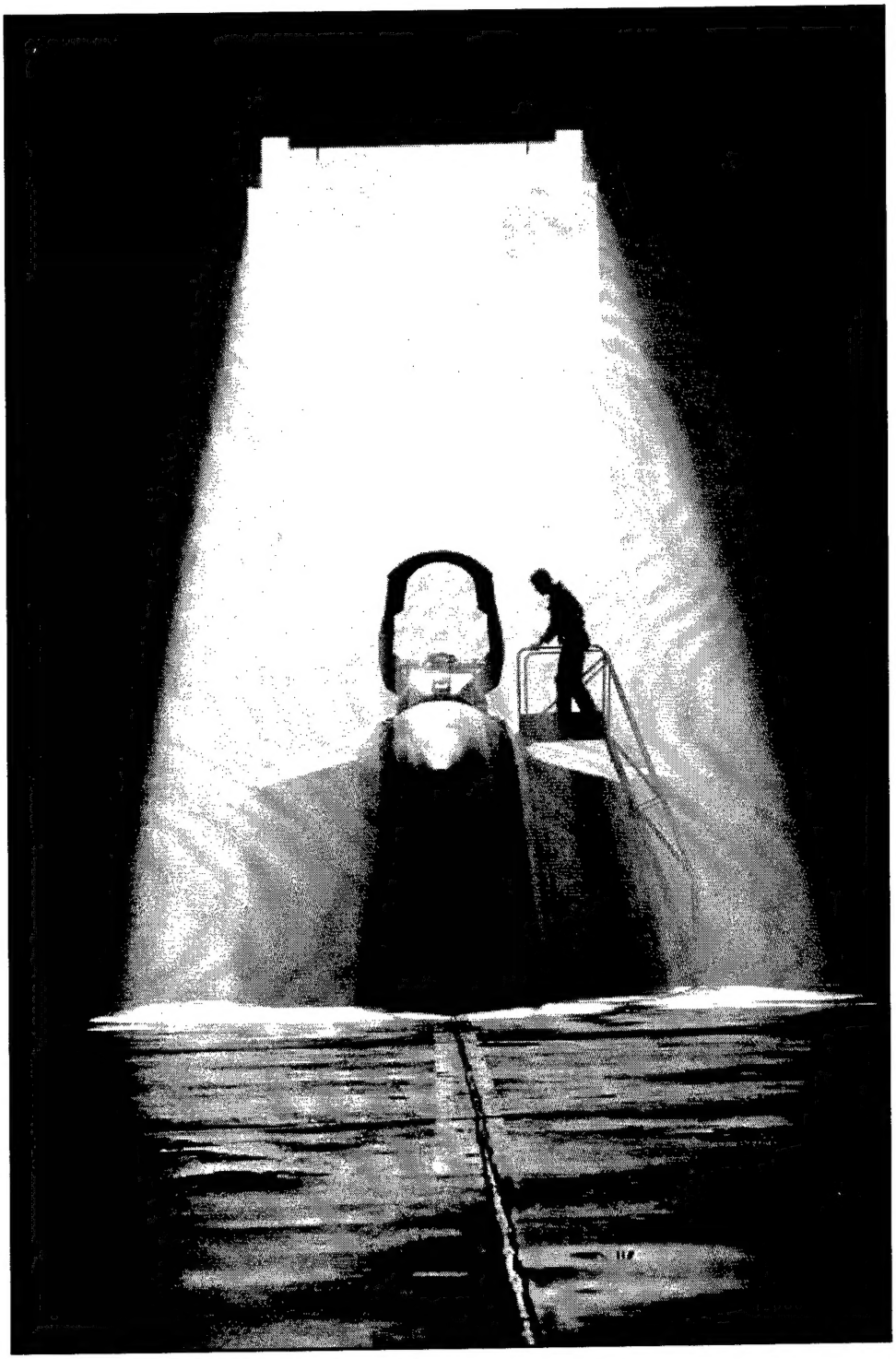
17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT

ACQUISITION Review QUARTERLY

Spring 2000
Vol. 7, No. 2

TABLE OF CONTENTS

OPINION



CYBER WARFARE: PROTECTING MILITARY SYSTEMS

Lt Col Lionel D. Alford, Jr., USAF

Software is a key component in nearly every critical system used by the Department of Defense. Attacking the software in a system—cyber warfare—is a revolutionary method of pursuing war. This article describes various cyber warfare approaches and suggests methods to counter them.

Karl von Clausewitz (1996) defined war as "...an act of violence intended to compel our opponent to fulfill our will... In order to attain this object fully, the enemy must be disarmed, and disarmament becomes therefore the immediate object of hostilities...." At the end of the second millennium, this definition no longer describes the full spectrum of modern warfare. In the future, we will have the potential to make war without the use of violence and fulfill the second half of von Clausewitz's definition—with software alone. Today's software-intensive systems make this possible.

"Cyber" describes systems that use mechanical or electronic systems to replace human control. In this article the term includes systems that incorporate software as a key control element. Cyber warfare can be executed without violence, and therefore the dependence on software-intensive systems—cyber systems—can make nations vulnerable to warfare without violence.

From Protecting Information to Protecting Software-Controlled Systems

Cyber warfare is the conduct of military operations according to information-related principles (Arquilla and Ronfeldt, 1992). This does not define the full degree of capabilities now possible in cyber warfare. Limiting the scope of cyber warfare to "information-related principles" does not describe what happens when an enemy disrupts the electrical power grid of a nation by hacking into the controlling software (Figure 1). Information is not only

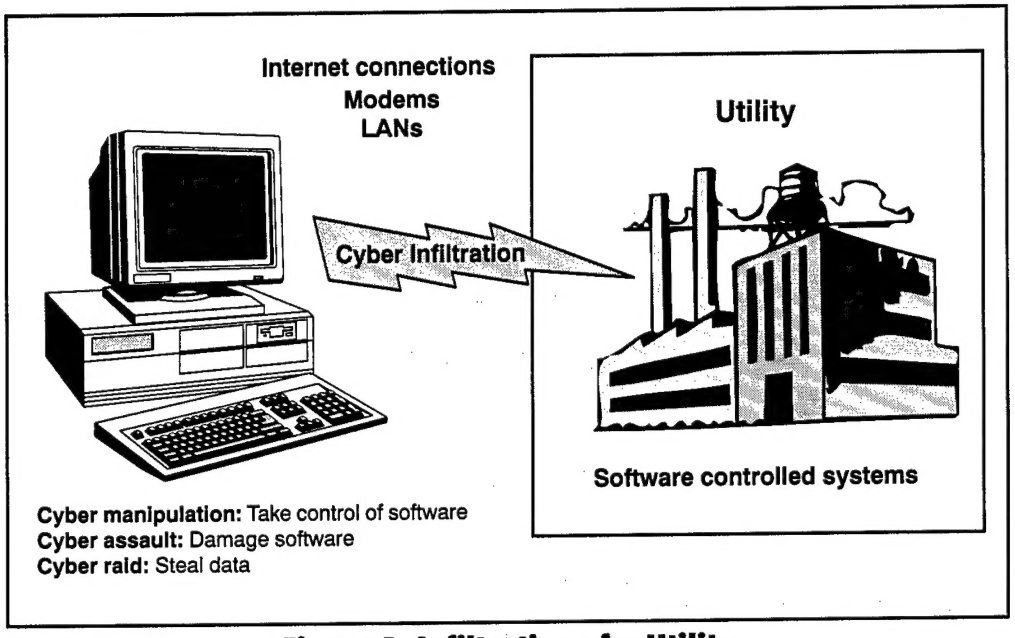


Figure 1. Infiltration of a Utility

at risk—the fundamental control of the civilization is. As technology pro-gresses, this "fundamental control" will devolve into networks and software-controlled electronics (Vatis, 1998).

This transition has already occurred in aviation. In the past, 100 percent of an aircraft's performance and capabilities were defined by hardware—the physical makeup of the aircraft. Today in the most advanced aircraft, 75 percent or more of the aircraft's performance and capability is absolutely dependent upon the software (U.S. Air Force, 1992). Without software, aircraft would not be controllable or reach the desired performance capabilities.[1] In some cases, through software, aircraft performance is gaining limited independence from physical configuration.[2]

Software dependence and hardware independence are growing. For example, modern aircraft fly by wire, their engines are controlled by wire, and their weapons are fired and dropped by wire. Systems that in the past were entirely hardware with mechanical control are being replaced by software with software control. Software defines the strength of modern systems, and provides a basis for the integration of many disparate items through networking. These networked software systems are under attack today, and the attacks are increasing (Figure 2).

Current Department of Defense (DoD) doctrines and instructions do not adequately cover the scope of cyber warfare (Stein, 1995). The following all handle information warfare as a discrete part of a military system: Joint Publication (JP) 3-13, "Joint Doctrine for Information Operations"; JP 3-13.1, "Joint Doctrine for Command and Control Warfare"; and instructions such as DoD 5000.2-R, "Mandatory Procedures for Major

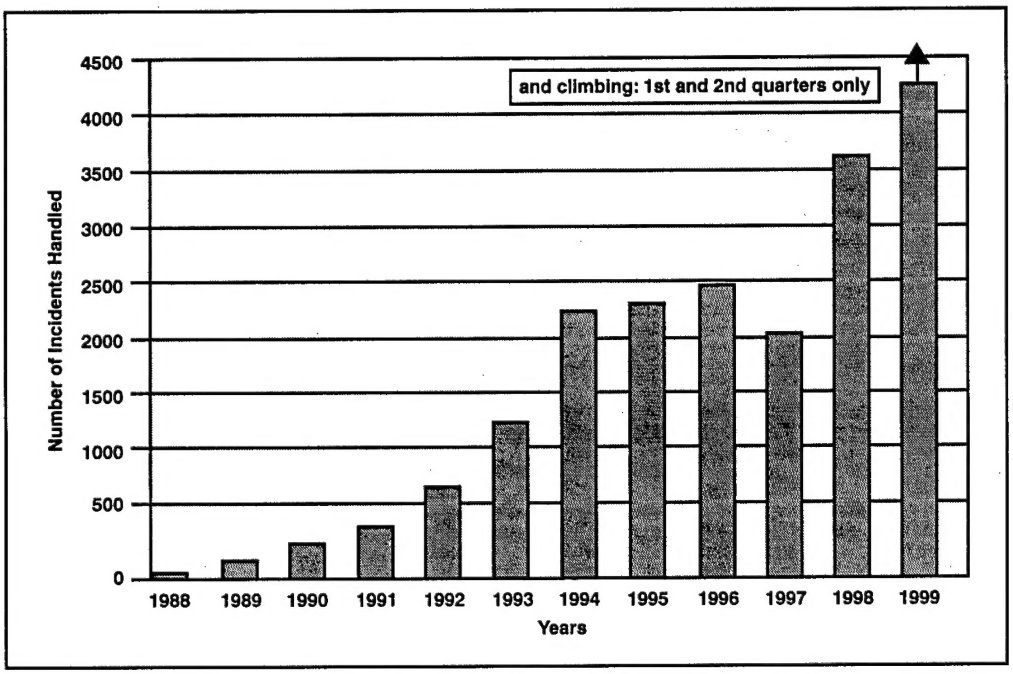


Figure 2. Number of CERT Incidents Handled

Defense Acquisition Programs (MDAPs) and Major Automated Information System (MAIS) Acquisition Programs." Current doctrine does not address software as the major element of a military fighting system; yet as the above discussion shows, many software and software-controlled systems cannot be separated from the system being developed.

The F–22 weapon system is an example of a software-controlled aircraft system that contains and communicates with integrated information systems (Figure 3). The F–22 is not a closed system; external information systems update and integrate F–22 combat operations during flight. Through these external connections, not just the information systems but the basic software systems of the F–22 can be attacked. Current information warfare doctrine in the Joint Pubs is mainly concerned with security of external C^4I (command, control, communications, computers, and intelligence) systems integrated on the F–22, but software-intensive systems make internal systems of the F–22 vulnerable to cyber warfare attack. Our doctrine must account for these vulnerabilities and provide methods of offense and defense. Definitions for building future weapon systems and in cyber forces doctrine and recommended methods to incorporate them follow.

Cyber Warfare Definitions

JP 3-13, JP 3-13.1, and DoD 5000.2-R focus on information systems and not software-controlled systems; definitions these documents provide are not sufficient to describe the full range of cyber warfare.

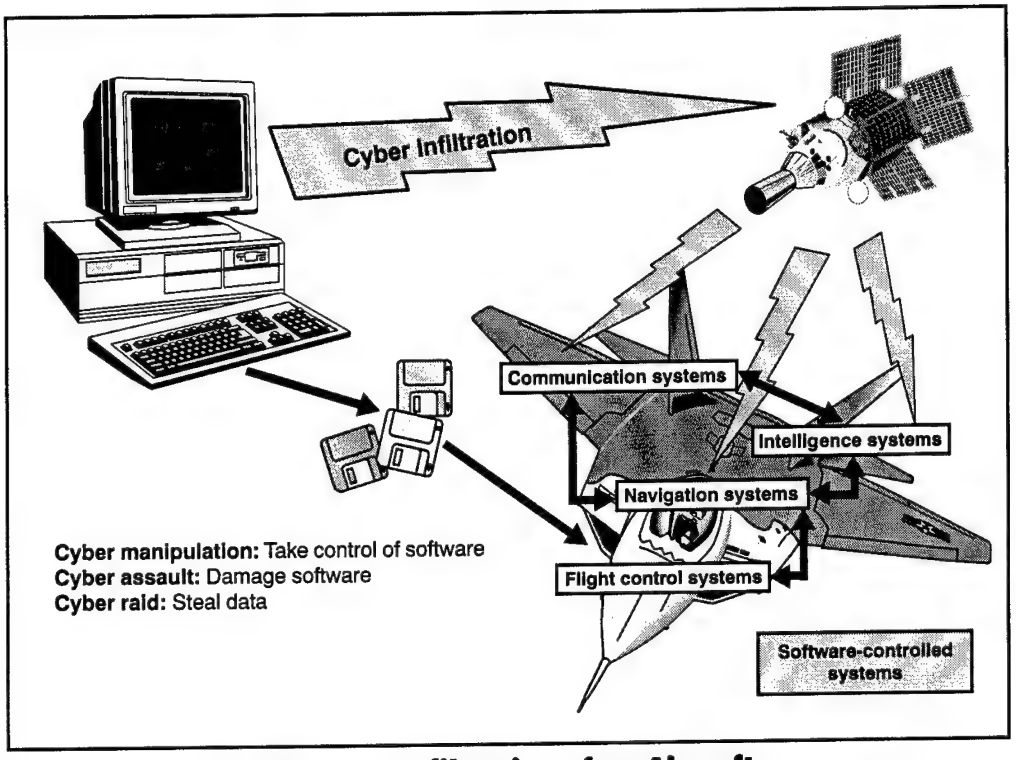


Figure 3. Infiltration of an Aircraft

The CERT® Coordination Center does provide a strong set of common terms to define cyber system security for the DoD (Carnegie Mellon, 1997), but these terms do not discuss military doctrine or national security. Furthermore, these terms focus on current methods of defense against infiltration and attack; they do not focus on future cyber force capabilities. We need a new taxonomy that includes the full range of cyber operations, and aids the development of a national cyber warfare doctrine (see adjacent box).

Military Cyber Warfare Targets

Any military system controlled by software is vulnerable to cyber attack. The first step in any attack is cyber infiltration; all systems that incorporate software are vulnerable to cyber infiltration.[4] Actions following cyber infiltration can affect organizations via the transfer, destruction, and altering of records—cyber raid. Software within systems can be manipulated—cyber manipulation. Systems controlled by that software can be damaged or controlled—cyber manipulation. The software itself can be copied, damaged, or rewritten—cyber assault.

Military C⁴I

Military C⁴I systems are particularly vulnerable, and are the primary focus of DoD cyber-related doctrine. JP 3-13 and JP 3-13.1 both provide doctrine for information-related warfare. C⁴I systems are a

A New Taxonony of Cyber Terms

Cyber warfare (CyW). Any act intended to compel an opponent to fulfill our national will, executed against the software controlling processes within an opponent's system. CyW includes the following modes of cyber attack: cyber infiltration, cyber manipulation, cyber assault, and cyber raid.

Cyber infiltration (CyI). Penetration of the defenses of a software-controlled system such that the system can be manipulated, assaulted, or raided.

Cyber manipulation (CyM). Following infiltration, the control of a system via its software which leaves the system intact, then uses the capabilities of the system to do damage. For example, using an electric utility's software to turn off power.

Cyber assault (CyA). Following infiltration, the destruction of software and data in the system, or attack on a system that damages the system capabilities. Includes viruses and overload of systems through e-mail (e-mail overflow).

Cyber raid (CyR). Following infiltration, the manipulation or acquisition of data within the system, which leaves the system intact, results in transfer, destruction, or alteration of data. For example, stealing e-mail or taking password lists from a mail server.

Cyber attack. See CyI, CyM, CyA, or CyR.

Cyber crime (CyC). Cyber attacks without the intent to affect national security or to further operations against national security.

Intentional cyber warfare attack (IA). any attack through cyber-means to intentionally affect national security (cyber warfare) or to further operations against national security. Includes cyber attacks by unintentional actors prompted by intentional actors. (Also see "unintentional cyber warfare attack.")

IA can be equated to warfare; it is national policy at the level of warfare. Unintentional attack is basically crime. UA may be committed by a bungling hacker or a professional cyber criminal, but the intent is self-serving and not to further any specific national objective. This does not mean unintentional attacks cannot affect policy or have devastating effects (Vatis, 1998).

Intentional cyber actors (I-actors). Individuals intentionally prosecuting cyber warfare (cyber operators, cyber troops, cyber warriors, cyber forces).

Unintentional cyber actors (U-actors). Individuals who unintentionally attack but affect national security and are largely unaware of the international ramifications of their actions. Unintentional actors may be influenced by I-actors but are unaware they are being manipulated to participate in cyber operations. U-actors include anyone who commits CyI, CyM, CyA, and CyR without the intent to affect national security or to further operations against national security. This group also includes individuals involved in CyC, journalists, and industrial spies.[3] The threat of journalists and industrial spies against systems including unintentional attacks caused by their CyI efforts should be considered high.

Unintentional cyber warfare attack (UA). Any attack through cyber-means, without the intent to affect national security (cyber crime).

very complex mix—from radios to radars, mainframes to personal computers. Military C⁴I uses interfaces through the Internet, base and organizational local area networks (LAN), modems, civilian and military communication systems, navigation systems, and radios in all frequency ranges.

Military C⁴I systems are extremely vulnerable because they interconnect. Cyber infiltration can enter at many points and potentially affect a myriad of systems. These systems and their interactions are so complex that any modern military organization is unlikely to trace the full potential of any single cyber infiltration. The possibility exists for cyber attacks of every type, and the results can be catastrophic. For instance, nuclear weapon control systems are incorporated into military C⁴I. As demonstrated by recent incursions in DoD networks, databases, and Web sites (Lemos, 1998), almost any dedicated foe can engage in cyber attacks against military computer systems (Vatis, 1998). Since military computers are the core of national C⁴I, successful IA and UA against such targets pose a national security peril.

"The possibility exists for cyber attacks of every type, and the results can be catastrophic."

Weapon Systems

No current DoD doctrine adequately covers cyber attacks on military hardware systems such as aircraft and vehicles that require software to operate (JP 3-13, 1998; JP 3-13.3, 1996; and DoD 5000.4-R, 1998). As noted previously, the F–22 is a cyber-controlled aircraft (Figure 3). Infiltration and degradation of the aircraft's systems directly or via its C⁴I connections can be as devastating as shooting it out of the sky.

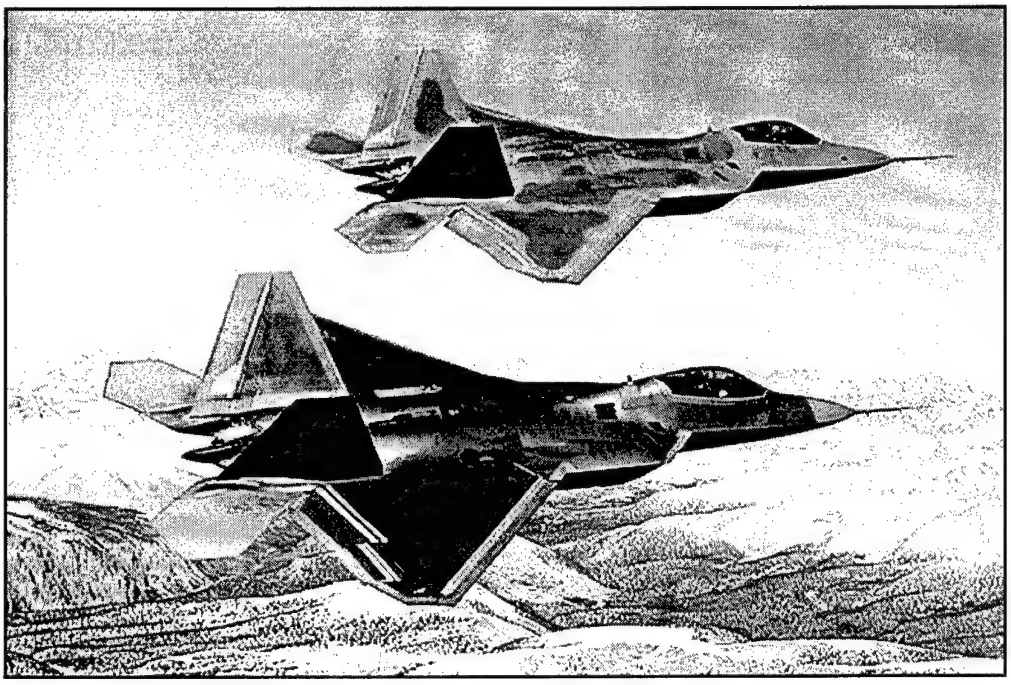
Cyber infiltration of the C⁴I system providing data to modern aircraft allows an avenue for cyber raid, manipulation, and assault. Because many systems like the Global Positioning System (GPS) automatically update aircraft information and intelligence, they can allow undetected infiltration of the aircraft. Intelligence, navigation, and communication systems are integrated to each other and input and output to a host of other aircraft systems—the flight control system (through the auto pilot), propulsion system (through the auto throttles), radar system, master warning system, and environmental control system. Using the correct control sequences, inputs, or reprogramming, an infiltrator could produce any level of systems damage, from driving the aircraft off course to overwriting the flight control software.

Identifying Cyber Warfare Vulnerabilities

The first rule in identifying cyber warfare vulnerabilities is that any software-controlled system that can accept an input can theoretically be infiltrated and attacked! This means all systems that accept inputs are vulnerable. Fundamentally, cyber systems can be infiltrated in two ways—by physical and signal inputs.

Physical Infiltration

Physical infiltration is made through the system hardware. For example, the on/off switch, keyboard, mouse, cockpit controls, flight controls, and removable



The F-22 is a cyber-controlled aircraft

media provide physical inputs into a system. The first line of defense for a software-based system is to secure the physical inputs and outputs of the system. If these are not secure, the system is not secure. Any system can be compromised if a cyber attacker can enter the facility, aircraft, or vehicle and directly infiltrate the system. The cyber infiltration can be maintained afterwards by the installation of repeaters and remote input devices on the hardware. For example, electronic bugs on phone lines are a common method of surreptitious surveillance; modem and LAN lines are equally vulnerable.

An easy method of physical infiltration is to use a spare LAN connection on a hub or route. Using common network parts, a connection can be made directly, or through a Radio Frequency (RF) transmitter (wireless connection) from the LAN to an infiltrator's computer. These infiltration methods are only discovered by careful system audits or visual inspection (Marshall, 1991).

Signal Infiltration

Signal infiltration comes through existing indirect or direct connections to a system. These connections are typically LANs, infrared (IR) devices, RF connections (radios), and modems (phone lines). Any system with an external connection can theoretically be infiltrated. The number of potential entry points is limited only by the number of direct and indirect connections into the system. For instance, a system with an Internet server is vulnerable to cyber infiltration from any computer connected to the Internet. An isolated network with a modem is vulnerable to any computer that can call

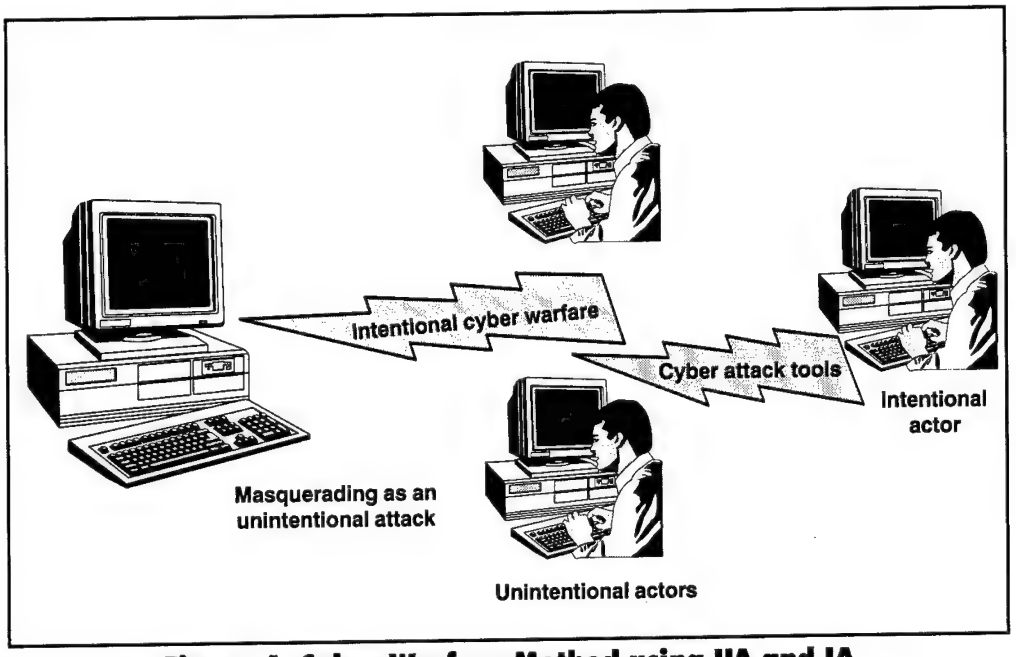


Figure 4. Cyber Warfare Method using UA and IA

into it. These input paths are used to infiltrate the system and then assault, manipulate, or raid it.

Physical infiltration may be protected by physical security: walls, fences, restricted areas, identification, guards, etc. Signal infiltration has similar defenses, but these are incorporated within the software or hardware itself (for instance, passwords, coded signals, firewalls, terminal identification, isolation, and system monitors).

The second rule of identifying CyW vulnerabilities is to expect every software-controlled system to be the objective of an attempted cyber infiltration. Even isolated systems can experience cyber assault through a computer virus brought in on a contaminated floppy disk. Because cyber attacks are largely unpredictable, all systems must have some degree of protection, and the level of protection must be commensurate with the likelihood and consequences of expected attack. Every vulnerable system needs proactive and effective virus-protection in place.

Assume U-actors will be influenced by I-actors. The anonymity of the Internet makes it possible for a cyber operative to pass on information about password-cracking, system phone numbers, infiltration techniques, and programs to U-actors (Figure 4). Many U-actors are young, immature, and unsophisticated. They don't understand the ramifications of their actions. However, some attacks that appear unintentional may be made by I-actors, operating through U-actors on the Internet. The recent cyber infiltration of information systems by California teens trained by the Israeli hacker "Analyzer" is an example of this mentoring relationship (Cole, 1998).

I-actors can easily influence the direction of attacks by providing system access

numbers and system passwords. Trojan horse programs written and passed to U-actors achieve an entirely different result than the U-actor intended. The outcome, from the perspective of the I-actor, is the same as if the attack had been made directly. Because passwords and infiltration data are shared by U-actors across the net, the I-actor's mission package is likely farmed out to more than one U-actor, or data may be passed through multiple U-actors. This ensures many attacks on the same target and further muddies the trail back to the source. This also means organizations that detect attacks and neutralize them should be prepared to receive the same attack over and over again. In addition, organizations that detect attacks must share data on the attacks immediately with other organizations (Howard, 1997).

Defense Against Cyber Warfare

The exploitation of system weaknesses and social engineering[5] are the primary avenues of attack against cyber systems (Howard, 1997). System weaknesses and social engineering techniques take advantage of computer and human limitations to steal and bypass signal and physical defenses, mainly passwords and machine-to-machine authentication. Unfortunately, the largest part of signal and physical defenses is based on identification and authentication codes—passwords. Passwords can be stolen, bypassed, or obtained by deception (and in theory, any password or authentication can be cracked). Until a different method of protection is invented, dependency on password identification and authentication guarantees that all systems will be in some degree vulnerable to cyber infiltration.

Use dedicated and redundant security to protect cyber systems. Twenty-two security methods are compiled below. Each method is described, along with some specific examples to accomplish it. This list is intended to provide a starting point for decision making and risk analysis; in some cases, especially systems integration and offensive methods, these suggestions run counter to current DoD policy and practice.

"Passwords can be stolen, bypassed, or obtained by deception (and in theory, any password or authentication can be cracked)."

These methods are intended to provoke thoughtful examination of all cyber security options to allow a tailored approach to military cyber systems development. To provide the best defense, these techniques must be customized, combined, and layered with one another. In every case, cyber systems should be set up so U- and I-actors can get into decoy sections[6] of the security network. This allows identification and containment of the infiltrator. Only when infiltration is identified can it be solved.

Inactive Defense Methods

Physical security is the primary means of cyber system protection. Without some degree of physical security, all of the defenses mentioned below will fail.

Isolate all critical systems. Provide no system inputs outside of a physically

secure area. Many agencies handle classified systems this way (Federal Information Processing Standards [FIPS] Publication 112, 1985); the systems themselves are physically isolated from any other inputs or systems. Isolation of critical systems also reduces damage caused by cyber infiltration.

Put critical operations under manual control. Critical functions should not be controlled directly by software. For example, an electrical power system should not be turned on or off through software. To be effective, the capability must be entirely eliminated from software control. For example, in a water utility, any setting that could cause water contamination should be manual so the system cannot be breached electronically. MIL-STD-882, "System Safety Program Requirements," is used by the military to classify critical functions. A basic rule for all critical cyber systems is that systems should be manual, when possible, so critical functions cannot be addressed by software. With industries such as nuclear power this is impossible; with military systems, this can be achieved by hardwiring critical functions—such as missile launches.

"All connections into a system must be physically controlled and monitored to prevent cyber infiltration."

Reduce integration. Integration increases cyber warfare risk because there are more avenues for cyber infiltration (and all system interconnections may not be known). To reduce cyber warfare vulnerability, integration should be limited as much as possible, and all system inputs and outputs must be fully defined. Critical cyber functions should be isolated physically so there are no inputs from outside. This type of compartmentalization should be considered when the use of cyber systems to control critical operations is necessary or desirable.

Keep the human element in the loop when integrating systems. Many software-controlled systems are integrated to reduce human workload. Although some systems require cyber integration to operate, many do not. When it is possible to keep a person in the loop or when a person can monitor or control a critical system, it is better to increase necessary monitoring and provide human interaction rather than automate the process. This is another way to isolate a system.

For instance, a request to shut down electrical power may generate a system message to tell a human operator to flip a switch. Only after the switch is moved can the automatic shutdown take place. An even safer setup would direct the operator through the shutdown sequence, instead of automating any of it. These methods may seem like we are turning back the technological clock, but protecting essential systems in this manner is necessary.

Inherent breach-points. Communication connections into the system are inherent, potential breaches of security. All connections into a system must be physically controlled and monitored to prevent cyber infiltration. The strongest breach-point occurs where the system is physically connected to an outside input. This part is also the most vulnerable to physical infiltration. Security must patrol, track, and control these inherent breach-points to prevent physical infiltration.

Active Defense Methods

These methods make up the software programming that protects the system from unauthorized use.

Passwords and authentications. Passwords and authentications are necessary parts of system security to allow authorized human and other cyber system input. Because personal passwords are not usually very long (10 digits is the standard maximum [FIPS Publication 112, 1985]), they are relatively easy to decode or predict. The longer the password, the better. Long passwords (32 characters or more) make code-breaking theoretically impossible, but codes that length are not commonly used and require other computers or hardware code devices such as tokens. Short passwords (eight characters or less) should be mixed into unpredictable, alphanumeric combinations and with other methods to provide an assured level of security. FIPS Publication 112, "Standard for Password Usage," provides specific information on the use of short passwords. Nicknames, popular words, and street names are easily predicted by some hacker programs.

Anthropomorphic measures. These measurements and data use a person's physical features—fingerprints, retinal scans, or face. These are better than passwords and can provide a much longer code, but are still relatively easy to break. Due to daily human physical changes, anthropomorphic measures cannot produce a large enough number to give a super-long password. For instance, if your face has swollen 0.001 of an inch during the night and the measure is to 0.0001 inch, you would not be able to log on your computer. However, anthropomorphic measures provide good security when combined with other methods such as passwords.

Tokens. These include magnetic cards or other code modules. They contain passwords and are read mechanically or electronically. Cards, modules, and other devices enable the use of very long codes and provide excellent security. Future encryption methods that use devices containing extremely long codes have the potential to make code-breaking almost impossible. A major drawback is that they must be kept physically secure because they can be lost or stolen. Tokens should be combined with anthropomorphic passwords to provide the best security.

"The first line of defense for a software-based system is to secure the physical inputs and outputs of the system."

Multiple authentications or log-ons. More than one interrogation is required to get into the system. For instance, log-on may require a basic password followed by an anthropomorphic measure (fingerprint, for example), or a password followed by a token. Figure 5 shows an example of this type of authentication scheme. The first layer should be a decoy layer and should be easy to crack but difficult to reprogram and disconnect. The second password layer should be very secure. Intrusions are recorded for investigation when the first layer is passed but the second layer is not. An infiltrator will invade the first layer, but not pass the second: then hopefully the infiltrator can be identified. In addition, the decoy layer can be filled with various offensive

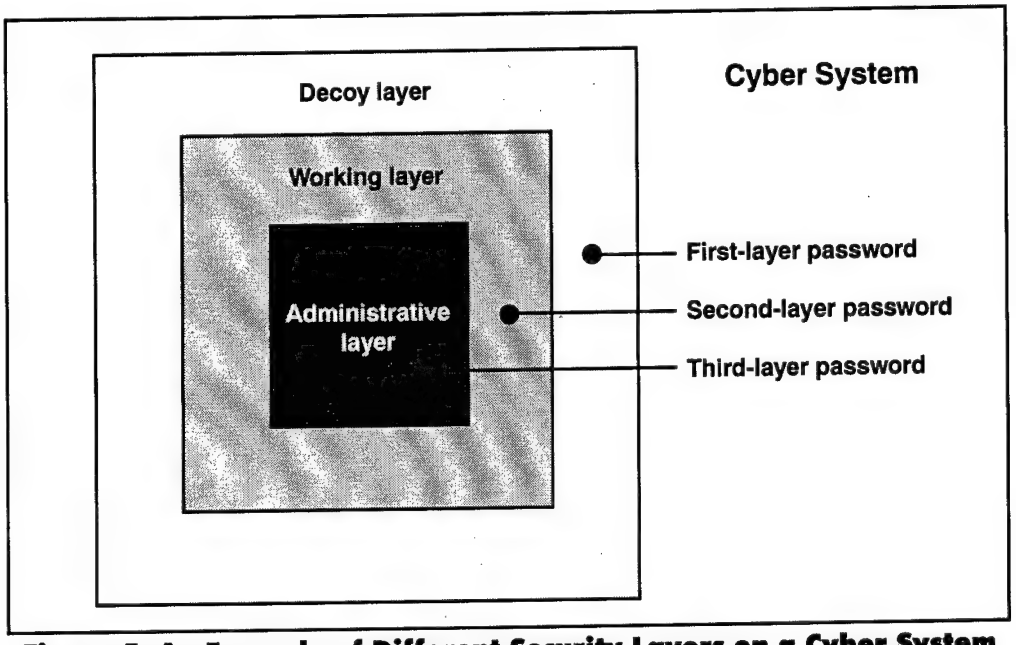


Figure 5. An Example of Different Security Layers on a Cyber System

programs that allow the identification and neutralization of the infiltrator. This type of log-on should be required for all vulnerable systems and especially for systems that interface with and support software-controlled aircraft and vehicles.

Multiple connection log-ons. More than one log-on over different addresses or lines is required for system entry. For instance, a log-on may be required at one phone number that activates a second, actual communication line. Another method is the call-back system. Using call-back, the user calls the computer and logs on, then the computer hangs up and calls back to the number authorized for the user. The user completes the sequence by logging on again with a second password. This method of log-on can also be used for Internet and LAN addresses.

Multiple log-on addresses. This requires either a call over two separate phone lines or two separate addresses at the same time. The signal is resolved in the user's computer only when both signals are received and the security authentication is passed on both lines. Multiple methods make it easy to detect cyber infiltration. Infiltrators who log-on in the initial layer, but whose second log-on fails, are instantly identified.

Monitoring software (Marshall, 1991). At the lowest level, this software records the user's activities on the system. In many systems, this software limits the user's access based on a security level. More complex systems monitor activity and alert the system or people monitoring when a user attempts to access resources not authorized at the user's security level. These programs provide audit trails and system logs that are a primary means of tracking unauthorized access and operations. This kind of software also detects multiple attempts at system log-on.

Active Offensive Methods

These methods include software programming and cyber operations that identify, attack, disable, tag, and capture I- and U-actors and their equipment. The chief problem to gaining the offensive is the detection of cyber infiltration. At least 75 percent or more cyber infiltrations are not detected (Howard, 1997). To an unsophisticated security system, cyber infiltration appears to be a normal connection. The security itself needs a footprint that is unpredictable to the infiltrator—that separates authorized from unauthorized operators. The techniques described in the previous Active Defense Methods section give some ideas how this can be accomplished.

This section provides methods that can be used against infiltrators after they are detected. Some of these techniques are theoretical and based on extrapolations of current program capabilities. Simple active programs (e.g., Microsoft macro viruses) and passive programs can be used against unsophisticated computer security and systems with crippling results. Commercially available system monitoring software can be used to accomplish cyber infiltration, assault, raid, and manipulation; to cyber infiltrate password-secured LANs requires only a rewrite of commercially available software.

Highly proficient programmers can write machine code programs that can be sent across a data stream into a Web browser or other communications program. For example, "Back Orifice" is a Trojan horse program that surreptitiously sends information through the Internet back to its originator. Most I-actors are not proficient enough to write these advanced programs, but simple offensive programs are available now on the Internet. Advanced programs can be written to do almost anything to a computer. They can tag a computer for identification (cookies), operate the different components of the computer, and rewrite programs in the computer.

Password-cracking programs. These were the first programs used for cyber infiltration. Password-cracking programs, at their simplest, repeatedly try different codes until they get a log-on. The main method of protecting against these simple programs is automatic monitoring that cuts off users who attempt multiple unsuccessful log-ons. Complex password cracking programs can potentially disable monitoring and other security methods. Super-long passwords and the defensive methods mentioned above protect against password cracking.

"Advanced programs can be written to do almost anything to a computer."

Identification, location, sniffer, spoofing, and watcher programs. Identification and location programs identify computers and users in a system. Sniffer and watcher programs glean passwords and other information from the system. Many of these programs are passive—that is, they are used by LANs to keep track of which computers and users are logged on. Some are active spoofers, actually asking for information from the user or the system.

The most widespread software-based method of obtaining passwords and other confidential information is through sniffer and watcher programs that monitor

network traffic. These are commonly deployed using Trojan horse programs such as "Back Orifice." Defeat these programs by applying the password encryption methods delineated in FIPS Pub 112 (1985). Sophisticated identification programs can make undetectable queries to the user's computer and even allow the cyber raid of data. The main line of protection from these programs is active-defense methods. Cyber protection systems should use covert identification programs to discover information about an infiltrator.

"As experiments, failure is not only allowed, it is a key aspect of success in allowing the system to be refined in the same environment it will ultimately be used."

Attack programs. An attack program is any program used to cripple or destroy a computer or computer system. These programs are complex and uncommon. They are like viruses, but are directed and singular, instead of random and replicating. Attack programs can be developed to impair the target's software, writable system basic input/output systems (BIOS),[7] and disks. When employed in defense, these programs should be used by cyber forces to immediately stop any cyber attack-in-progress, to prevent the infiltrator from continuing operations from the attacking computer. Any cyber attack should tag the system for identification.

Protection against direct attacks is best accomplished by defensive methods. However, because all parts of a network or the Internet may not be secure, each individual computer must have some way of independently identifying attacks and rejecting them. Similar methods are used extensively now to protect against viruses and reject cookies.

Tagging programs. These programs insert data on a computer for later identification and cyber infiltration. These programs can be as simple as a "cookie"[8] or as complex as a BIOS tag. Some versions write data to the boot sector on the hard drive; the drive must be low-level reformatted to remove it. Cyber forces should be able to tag a computer for later criminal investigation. Methods of defense from tagging are similar to those from attack programs.

Viruses. These are programs that replicate themselves by attaching their codes to other programs, disk boot sectors, and writable-system BIOSs. Viruses can be used both for malicious terrorism and cyber warfare (Symantic Antivirus Research Center, 1994). This capability can be added to any offensive program. It attacks computers in the opponent's system except for the primary infiltrator's computer. Virus capabilities can be added to tagging programs when there is a threat that the infiltrator will destroy the system or hard drives attacked, and thus attempt to prevent later identification. Because of their ability to get into nonopponent computer systems, viruses should be used cautiously by cyber forces. Viruses can be written with checks that only target specific systems.

Methods of defense from viruses are:

- programs that scan for identified viruses and virus-like code (virus scanners),

- inoculation of systems by identification of authorized programs and data (Cyclic Redundancy Code [CRC] records; many virus checkers provide this capability), and
- personnel training.

Unfortunately, by 1997 as many as 15,500 viruses were identified and an estimated 400 new ones are reported each month (Dr. Solomon Company, 1997). This makes absolute protection from viruses and viruslike programs impossible without the use of the defensive methods enumerated previously.

Trojan horses. These programs are the most common method of cyber infiltration (Howard, 1997). These are programs that perform like any other program a user may wish to run, but they execute unauthorized operations (Carnegie Mellon, 1997). A common example of a Trojan horse program is a Microsoft macro virus. Trojan horses can be defeated by the same methods used against viruses.

System overflows. One method of cyber infiltration and cyber assault is the use of large amounts of data to cause a system overflow or "crash." The typical e-mail pyramid letter is a crude example of e-mail overflow. This kind of letter can accumulate an address tail that will choke any e-mail system. A cyber attacker can also be attacked and infiltrated in this manner.

Overflows are most effective when the overflow is not detected immediately. This can be achieved when the infiltrator has a very fast connection or when there is a second signal input line to the attacking computer. Data overflows are also an excellent method to mask the transmission of offensive programs. Methods of defense from overflows are e-mail scanners that check for very large e-mail files, and personnel training. For instance, all personnel must be taught not to pass on dubious e-mail warnings, chain e-mails, and massive official e-mail. In addition, all employees should never open files from questionable sources or unofficial files.

Direct manipulation. When a computer is connected to another computer, current software makes it relatively easy to take control of many of the basic functions of the computer. Machine code and operating systems address codes can be used to turn on peer-to-peer sharing or to directly manipulate devices controlled through the operating system and BIOS. Cyber forces should develop programs that will allow this kind of manipulation of infiltrator computers. Cyber systems must lock out unauthorized system requests at all levels.

"One method of cyber infiltration and cyber assault is the use of large amounts of data to cause a system overflow or 'crash.'"

Logic bombs. Some code sequences in data files manipulate both the programs using the data files and the address codes of the BIOS and operating system. This is evident in macro viruses found in document files and files that result in program and operating system crashes. These kinds of programs can be written to achieve even more pointed results: for example, tagging or systems impairment. Logic bombs can also be used against infiltrators when they are attached to password data bases, classified data files, or to other files that might be downloaded following cyber infiltration.

Statutory action (legal actions). Cyber forces cannot be fully effective without capturing and prosecuting both U- and I-actors. The primary goal of offensive cyber operations must be to identify and tag infiltrating systems. These actions allow prosecution as well as confirmation of the infiltration. Because it is relatively simple to back up systems and replace damaged computer components, the infiltrator will not be out of action for long unless legal action is taken. When it is not possible to extradite and prosecute U- or I-actors outside the United States, national policy must determine the extent of the cyber operations to be undertaken against the shielding foreign nation.

"The primary goal of offensive cyber operations must be to identify and tag infiltrating systems."

Measuring the Effectiveness of Cyber Defenses and Operations

The effectiveness of cyber forces cannot be measured by a lack of detected cyber infiltration against targets This is because undetected cyber infiltration is certainly taking place (Lee, 1998), and most cyber infiltrations and attacks go undetected (Howard, 1997). The only reasonable measure of effectiveness is detecting cyber infiltration when it happens. This is why a multilayered approach to cyber system defenses is necessary. If the policy of the United States regarding CyW is wholly one of defense, the absolutely perfect measure of defense effectiveness is that every cyber infiltration is identified and the U- or I-actor neutralized.

The success of cyber operations against and in support of the U.S. government must be classified. As mentioned previously, when a cyber attack occurs, with due regard for active cyber operations, the detecting agency should immediately inform all possible targets (Howard, 1997). But, when an agent of the government is the victim of successful cyber infiltration or attack, that agency should not release the degree or effects of any cyber operation against it. Acknowledging the results would be similar to acknowledging the classification of publicly published materials. It would tell the enemy they are successful and provide information so the next attack might be even more effective.

The best approach is for the agency to make no comment at all and provide immediate recovery and cleanup as part of its cyber operations. This keeps the I- and U-actors guessing and allows the effective use of the offensive and defensive methods outlined above. This is not to say the agency should not report the attack to proper authorities and provide suggested methods of protection.

New Doctrine

The first step to develop a strong doctrine that includes all the dimensions of current and future cyber warfare threats. Taxonomy and cataloged security methods go a long way to build a framework for this doctrine. The challenge is to put the required effort and funding forward to ensure a strong level of security for all software-controlled systems.

CONCLUSION

Cyber operations have the potential to overcome any system controlled by software. The military systems we are developing today depend on software and software-controlled components to operate. Cyber warfare defenses must be incorporated into all of these military systems. The future of warfare makes it imperative that cyber warfare concerns become the interest of every software and hardware developer—not only of military systems but civilian systems as well.

Cyber warfare may be the greatest threat that nations have ever faced. Never before has it been possible for one person to potentially affect an entire nation's security. And never before has one person had the ability to cause such widespread harm as is possible in cyber warfare. Like radioactive fallout, the affects of cyber warfare can devastate economies and civilizations long after the shooting war is over.

This genie can' t be put back into the bottle; societies will not want to give up the manifold prosperity brought about by cyber systems. But a nation must ensure that it maintains the upper hand in cyber warfare. If our nation can' t, then even with the most powerful military and defense economy in the world, we face an insurmountable threat to our future prosperity and security.

Lt Col Lionel D. Alford, Jr., U.S. Air Force, is an aeronautical test policy manager for the Headquarters Air Force Materiel Command, Wright-Patterson Air Force Base, OH. He is an Air Force experimental test pilot with more than 3,600 hours in more than 40 different kinds of aircraft and is a member of the Society of Experimental Test Pilots. He is a graduate of the Air Ground Operations School, the Combat Aircrew Training School, the All Weather Aerial Delivery Training School, Defense Systems Management College, and the U.S. Air Force Test Pilot School. He has a master's degree in mechanical engineering from Boston University and a bachelor's degree in chemistry from Pacific Lutheran University.
(E-mail address: Pilotlion@aol.com)

References

Arquilla, J., & Ronfeldt, D. (1992). Emergent modes of conflict. In *Cyberwar is coming.* Santa Monica, CA. The RAND Corporation.

Carnegie Mellon. (1997). *Glossary of terms.* Software Engineering Institute, CERT® Coordination Center. http://www.cert.org/research/JHThesis/appendix_html/Glossary.html

Cole, R. (1998). FBI hunts "master hacker." ABC News: High Technology, The Associated Press.

DoD 5000.2-R. (1998, February 27). Mandatory procedures for major defense acquisition programs (MDAPs) and major automated information system (MAIS) acquisition programs.

DoD Joint Publication (JP) 3-13. (1998, October 9). *Joint doctrine for information operations.*

DoD Joint Publication (JP) 3-13.1. (1996, February 7). *Joint doctrine for command and control warfare.*

Dr. Solomon Company. (1997). The future impact of viruses. *Dr. Solomon's Virus Central.* http:/www.drsolomon.com/vircen/vanalyse/future.html

Federal Information Processing Standards (FIPS) Publication 112. (1985). Standard for password usage.

Hafner, K. (1998, July 23). Chiquita case illustrates vulnerability of voice mail. *New York Times.* http://www.nytimes.com/library/tech/98/07/circuits/articles/23voic.html

Howard, J. D. (1997). *An analysis of security incidents in the Internet 1989–1995.* Carnegie Mellon University. http://www.cert.org/research/JHThesis/Start.html

Lee, S. (1998). Most computer hackers go unnoticed. *South China Morning Post.* http://www.infowar.com/HACKER/hack_030198s_b.html-ssi

Lemos, R. (1998). DoD confirms hacker boast. *ZDNN.* http://www.zdnet.com/zdnn/content/zdnn/0421/309056.html

Marshall, V. H. (1991). Intrusion detection in computers. *Summary of the Trusted Information Systems (TIS) report on intrusion detection systems.* http://csrc.nist.gov/secpubs/auditool.txt

Stein, G. J. (1995, Spring). Information warfare. *Airpower Journal, IX*(1).

Symantic Antivirus Research Center. (1994). *Computer viruses—An executive brief.* http://www.symantec.com/avcenter/reference/corpst.html

Vatis, M. A. (1998). *Cybercrime, transnational crime, and intellectual property theft. Statement for the record before the Congressional Joint Economic Committee.* http://www.ilspi.com/vatis.htm

von Clausewitz, K. (1976). In M. Howard & P. Paret (Trans.), *On War* (Book I). Princeton, NJ: Princeton University Press.

U.S. Air Force (1992). Bold stroke. Executive Software Course.

ENDNOTES

1. The F-16 is unstable below Mach 1, and uncontrollable without its software-based flight control system. The Boeing 777 and the Airbus 330 have software flight control systems without any manual backup; the performance of these aircraft is dependent on their digital flight control systems.

2. The F–22 in high angle of attack flight uses software-controlled vectored thrust and flight controls to maneuver the aircraft.

3. As seen in allegations that a *Cincinnati Enquirer* reporter stole voice mail messages from Chiquita Brands International (Hafner, 1998), CyR is becoming a common method to take information from cyber systems.

4. The "hacker" is a U-actor commonly characterized as affecting cyber infiltration without further damage to a computer system.

5. Social engineering refers here to both the process of gaining privileged information, such as passwords, by deception (3) and the use of Trojan horse programs.

6. A decoy section is a first layer area of a cyber system that appears to provide access to the system but in fact only simulates the inner layers.

7. A basic input/output system is a set of instructions stored on a ROM chip inside IBM PCs and PC-compatibles, which handles all input-output functions.

8. A cookie is a set of data that a Web site server gives to a browser the first time the user visits the site, that is updated with each return visit. The remote server saves the information the cookie contains about the user and the user's browser does the same, as a text file stored in the Netscape or Explorer system folder. Not all browsers support cookies.

ENTERPRISE ARCHITECTURE FOR DOD ACQUISITION

CDR David P. Brown, USN

The Department of Defense (DoD) could achieve substantially higher acquisition cost savings by following the lead of industry in applying systems engineering theory to organizational structure, to develop an enterprise architecture for DoD acquisition.

The Department of Defense has made great strides within the past five years in moving defense acquisition processes toward successful business practices. Despite the undeniable successes achieved, acquisition reform has the potential to achieve substantially more costs savings than have to date been realized. These potential savings must be achieved if the services are to be able to modernize for tomorrow's operational demands.

Much of the equipment used by our warfighters is old, and gets older each day. The costs associated with supporting these systems are increasing with time. Although it appears that continued reductions in defense procurement budgets may level off and may actually increase in the coming years, more procurement dollars will be needed to meet the needs of the services. Jacques Gansler, Under Secretary of Defense for Acquisition, Technology, and Logistics (USD [AT&L]), has continually spoken of the need to generate the dollars necessary to modernize forces while continuing to meet the operations and maintenance demands of high operational tempos.

Where will these funds come from? The premise of this article is that DoD could achieve substantially higher acquisition cost savings by following the lead of industry in developing an enterprise architecture for DoD acquisition. Commercial corporations have discovered that efficient business processes must be carried out within streamlined, seamless organizational structures. To achieve higher cost savings, DoD must reengineer its organizational structure. This will require a change in focus from optimizing individual departments and functions toward a top-down approach that focuses on optimizing the DoD acquisition system at the highest (enterprise) level.

The proposed solution is the development of an enterprise architecture for DoD

acquisition. Enterprise architecting is the application of proven systems engineering principles for integrating complex systems applied toward integrating complex organizations. Most large corporations have realized that they cannot be effective and survive the commercial marketplace unless they develop an architecture for their organization that provides a seamless integration between different elements of the corporation. The larger and more complex the organization, the more critical this is. When subsystems of either a physical or organizational system are not designed to be interoperable with seamless operation across the interface, an "architectural mismatch" occurs and poor system level performance results.

"Systems engineering was developed as a process to design systems from the top down."

Enterprise Architecture

What is an enterprise architecture? By the definition of John Zachman, "Architecture is that set of design artifacts, or descriptive representations, that are relevant for describing an object such that it can be produced to requirements (quality) as well as maintained over the period of its useful life (change)" (Zachman, 1991, p. 4). An enterprise architecture is developed by applying this concept to the organizational, or enterprise, level of a company or organization. This can be accomplished by applying many of the tools of systems engineering to the engineering of an organizational structure.

The discipline of systems engineering came about as industry began to develop complex systems and products. Engineers realized that having specialists first design and build optimized components and then attempt to integrate them resulted in poorly performing systems. This method was also time-consuming and expensive as many components required extensive redesign and rework to get them to be interoperable. Furthermore, the voice of the customer was often lost in the pursuit of optimum performance at the subsystem level.

Systems engineering was developed as a process to design systems from the top down. The system level architecture is defined first. Subsystems and components are then designed to support the system requirements and to be interoperable with other components and subsystems. In many cases, this requires that the individual subsystems or components be suboptimized. However, the result is a better overall system that can be developed faster and at a lower cost.

Many large, complex corporations have realized that this same principle applies to the architecture of an organization. Most corporations have traditionally been organized around functional areas such as marketing, accounting, engineering, and public relations. In most cases, these functional departments were designed to be the most efficient at the functional task they performed. This has led to efficient departments that combine to produce dysfunctional organizations.

The epitome of this type of structure is satirized in the cartoon strip "Dilbert." Dilbert attempts to do his job amidst insurmountable trials and tribulations: Research won't give him the product

requirements, accounting reduces his budget, his boss tells him to get started without the requirements so he looks busy to upper management, and on and on. Why is the "Dilbert" cartoon strip so popular? Probably because so many of us can relate to these issues in our daily jobs.

Major commercial companies are realizing that this type of functional behavior is inefficient and wasteful, and that it threatens their future survival in the global marketplace. They are developing enterprise architectures to integrate their organizations and provide a clear vision of where they are headed in the future.

A good analogy of the process involved in developing an enterprise architecture is a city planning commission. These commissions make zoning laws, review building plans and permits, manage building codes, and grant deviations on a case-by-case basis. They monitor demographics, economics, changes in technology, and attitudes in the community. For a city to operate effectively, the commission must balance the conflicting priorities and goals of diverse groups such as its citizens, builders, businesses, and employees. Interfaces between these conflicting groups must also be managed so that the best interests of the city as a system are achieved. The process must also be responsive to change.

Why does enterprise architecting play such a large role in commercial companies? In 1967, 40 to 50 percent of the cost of a product was direct (touch) labor. Today that percentage is as low as 15 percent. At the same time, between 20 and 50 percent of all labor cost in the United States is now dedicated to gathering, storage, retrieval, reconciliation, and reporting of information used to run the company (Zachman, 1997, pp. 8–10).

Because of the functional organization of most companies, this task is being accomplished with horrible inefficiencies. Larry English of Information International has observed that 70 percent of computer printouts were used to enter the same data into a different database. Bill Smith of William G. Smith Associates has observed that 70 percent of the lines of code used by a company are doing nothing but moving data from system to system and 40 percent of machine cycles are expended moving data that produces no useful work. At a cost of $1 to $4 per line of code for Y2K correction and testing, the price tag to ensure that these programs are now working is in the hundreds of billions of dollars. Statistically, the average data fact is stored 10.8 times within a company information structure (Zachman, 1997, pp. 8–10). Since DoD is heavily engaged in generating and using information (rather than producing physical products), our percentages are likely worse than our commercial counterparts.

"A good analogy of the process involved in developing an enterprise architecture is a city planning commission."

Figures such as these are bound to capture the attention of any chief executive officer. As Doug Erickson remarked, "Where do you think management is going to get any more major chunks of cost reduction? It looks to me like these enormous costs of architectural discontinuities and redundancies are now the 'low hanging fruit' just waiting to be

picked" (Zachman, 1997, p. 10). The best part of the enterprise architecture is that up-front investment is minimal compared to other cost-saving initiatives, such as automation. Like systems engineering, much of this is just a commonsense approach to doing business. The difficult part will be to smash down the walls of functional bureaucracy in implementing these changes.

Some may argue that DoD is already embarked on development of an enterprise architecture through implementation of the "joint technical architecture" and other standardization initiatives. It is certainly true that these initiatives will increase interoperability between functional groups and organizations through improved design practices. However, this effort falls far short of the organizational change required to achieve a seamless, integrated acquisition organization. In business process reengineering, the first rule is to optimize the process before considering how to automate it.

In enterprise engineering, the issue is not how to make a functional group more efficient, but how to make the organization the most efficient. Instead of initiatives to make the travel section more efficient, the more appropriate question is, do we even need a travel section? Perhaps the organization would be better served by placing travel service functions on the corporate Intranet and having employees make reservations and enter claims data directly into the system. Many current acquisition reform initiatives fall into the category of continuing optimization of functional areas, for example, in improved contracting processes and improved design practices. To achieve the full potential of the reform initiative, we need to focus more on optimization at the enterprise level.

Table 1. Zachman Framework[a]

	Data *What*	Function *How*	Network *Where*	People *Who*	Time *When*	Motivation *Why*
Scope: ***Planner***						
Enterprise model: ***Owner***						
System model: ***Designer***						
Technology model: ***Builder***						
Detailed representations: ***Subcontractor***						

[a] From Zachman (1997, p. 5).

Zachman Framework

How can DoD develop an enterprise architecture? The most applicable approach to enterprise architectures for DoD I have found is the Zachman framework (Table 1). John Zachman worked in information systems for airframe manufacturing in the early 1970s. He developed his enterprise architecture when he realized that the same principles of systems engineering used to engineer complex physical systems could be applied to engineering large, complex organizations. These important elements included a clear understanding of requirements (goals of the organization), seamless internal and external interfaces, prudent managed risk taking and managed change. He developed enterprise engineering to accomplish these goals.

Like systems engineering, enterprise engineering takes a top-down approach toward development of the enterprise structure. DoD acquisition would fit the Zachman framework outlined in Table 1 as follows: The Office of the Secretary of Defense (OSD) would be the planner (row 1). The owner is the user of the system (row 2). The designer is the acquisition program office; the builder is the prime contractor of the system; and the subcontractors (row 5) would be subcontractors to the prime. The columns of the Zachman framework then ask the questions: what, how, where, who, when, and why. Filling in the process model in each block and then coordinating the interfaces between each would provide the DoD acquisition architecture, ensuring that all necessary functions are addressed, that the functions performed at each level are defined and understood, and defining the relationships between levels.

The Zachman framework provides an excellent template for developing the architecture of just about anything. However, Zachman left out one important aspect of systems engineering in his framework that would be essential to implementing an enterprise architecture in DoD. Metrics is an important element of tracking progress toward achieving a goal in any endeavor. I would therefore recommend that one additional column be added to the framework labeled "progress." This would be the metric that provides the key measure of success toward achieving the "what" of column one.

"Like systems engineering, enterprise engineering takes a top-down approach toward development of the enterprise structure."

Applying the Zachman Framework to DoD

The Zachman framework can make important contributions to acquisition reform. Policy makers have focused on the what, how, where, and when of what has to be done. They have done little to identify the who or the why. A key part of the systems engineering process is the assignment of responsibility and metrics to track progress toward achievement of the goals. Another key is providing the motivation of column 6 to accomplish the goal.

In a recent speech at the Defense Systems Management College, Vicky Farrow, chief learning officer of Lucent Technologies, Inc., described how demanding good personal performance on the job was a major part of Lucent's rise from single-digit growth as a part of AT&T to growth rates in the 20th percentile as an independent company (1999). She described how one employee was interviewed and asked what her job was. The woman explained that her job was to go to job fairs and to talk to students about working at Lucent. When asked how many students to which she had spoken put in applications, she said she had no idea.

Commercial industry has realized that each person must understand the goals of the company and the part their particular job plays in the achievement of those goals. To make sure that these individual linkages are defined, top companies provide personal incentives to their workers. These can take the form of bonuses for exceptional achievement or removal for consistent substandard performance. How many DoD employees do we have that are like this woman? They go to work every day and perform their work with little or no understanding of the relationship between their jobs and the higher level goals of supporting the warfighter or achieving the goals of acquisition reform.

"Establishing motivation is more difficult in DoD because of many rules for paying and firing government employees."

Establishing motivation is more difficult in DoD because of many rules for paying and firing government employees. But there are certainly some personal motivations that could be put in place under existing law. For example, to reduce development time, OSD might assign responsibility to a senior executive service (SES) employee to reduce the time to get through a milestone decision by 50 percent over three years. Times would be measured and tracked and the SES's bonus would be directly tied to the achievement of the intermediate goals for each year.

Developing an Enterprise Architecture

An overview of the enterprise architecture planning process is presented in Figure 1. Following the top-down approach of systems engineering, this process layers out four phases of planning for the implementation of an enterprise architecture. The four steps of planning corresponding to the four levels above ask (Spewak, 1993, p. 14):

- Where do we start?
- Where are we today?
- Where do we want to be in the future?
- How do we get there?

By answering these questions and filling in the Zachman framework, the outline of the enterprise architecture is formed.

Another area in which the Zachman framework could be applied to DoD acquisition is the identification of the interfaces between the various rows of the

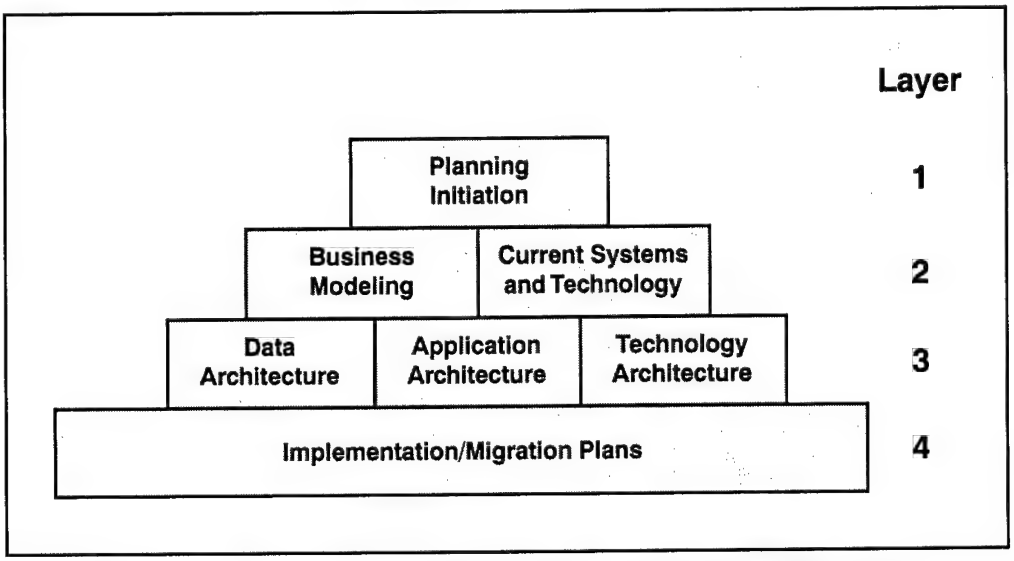


Figure 1. Components of Enterprise Architecture Planning

framework. Some progress has been made in improving the interface between the user and acquisition communities. The Joint Strike Fighter program was able to integrate the user into the program management structure through the integrated product team (IPT) process.

By assigning a group of users to the program office staff to work with the many stakeholders in the Air Force, Navy, and Marine Corps, the users worked side by side with the acquisition community in scheduling, risk analysis and assessment, budgeting, and all other facets of program management. They received training in program management like their acquisition corps counterparts. They used structured methods such as quality function deployment (QFD) to trade requirements not just for performance, but across a broad range of acquisition issues such as cost, producibility, logistics supportability, and development schedule. Requirements were rigorously scrubbed by running them through a variety of modeling and simulation tools to validate whether a requirement actually produced a measurable benefit. They motivated the services to send the best and brightest by providing joint duty credit (a requirement for flag officers) for those that served in the billets.

Unfortunately, this initiative cannot be repeated across all programs. There are not enough users to assign them full time to every program office. However, using the Zachman framework, some of the underlying principles of the successes achieved in this pilot program should be transferable. These include training of requirements writers in basic acquisition policy, operational requirements document development through an IPT process including all stakeholders, use of structured methods, requirements validation through simulation-based acquisition tools, and a system that recruits the best and rewards those that perform well.

Implementing an Enterprise Architecture in DoD

Successful implementation of enterprise architectures is difficult to accomplish in any setting. Many efforts in the commercial sector have failed for reasons common to any endeavor to institute change. These include a lack of management acceptance, failure to motivate personnel to cooperate, focus on short-term gains, political differences over responsibility, and lack of resources. Implementing a seamless acquisition process within DoD will be extremely difficult in that it directly conflicts with the first law of bureaucracy, which states: "The first priority of a bureaucracy is the preservation of the bureaucracy."

"Successful implementation of enterprise architectures is difficult to accomplish in any setting."

Much of the increased efficiency achieved in the commercial sector has been done by targeting middle management in restructuring and downsizing. The recent Government Accounting Office (GAO, 1996) report on downsizing shows that government organizations have protected managers while downsizing workers. Industry has generally found that the use of outside consultants was necessary to achieve a more efficient organization when downsizing. This suggests that development of a DoD enterprise architecture should be done with the assistance of outside consultants.

Overcoming resistance to change should not be underestimated. The commercial sector has also found it difficult to implement major changes to the way they do business. Implementing major changes sometimes requires development of a totally new organization. General Motors created the Saturn division because they could not institute the required changes to automobile manufacturing within their union plant structure. Lucent Technologies achieved their threefold increase in growth after being created as a spinoff company of AT&T Corporation. DoD has also experimented with small, independent organizations to implement totally reengineered business processes in place of large, existing bureaucracies.

The Joint Advanced Strike Technology Program (currently the Joint Strike Fighter) was created to operate outside the Air System Commands of both the Navy and the Air Force. To date, it has successfully operated with a much smaller, leaner office structure than comparable aircraft development programs. Creation of small, spinoff operations operating outside the normal functional bureaucracies appears to be a successful method of instituting reengineered organizations at a much more rapid pace than incremental change within large, established organizations.

Conclusions

Commercial industries are realizing that the best opportunities for reducing costs are in the architectural mismatches that exist within their corporations.

Realizing these cost savings will be essential to survival in a global economy. DoD must find new ways to achieve the cost savings necessary to replace the numerous aging systems throughout all service branches. Development of an enterprise architecture including seamless interfaces between each level, assignment of responsibilities, metrics for measuring success, and personal accountability for results could be a substantial contributor to achieving the needed efficiencies and cost savings. The Zachman framework, with the addition of a metrics column, provides the best template for defining an enterprise architecture for DoD.

Implementing the enterprise architecture will be the most difficult challenge, as it will require imposing change on entrenched bureaucracies. Transferring responsibilities to reengineered, smaller organizations is one proven method of achieving rapid change on a large scale. The question is not if DoD will follow the lead of industry, but when. John Zachman (1997, p. 11) expressed it best when he said, "My opinion is, we are on the verge of seeing architecture 'come into its own,' and in the 21st century, it will be the determining factor, the factor that separates the winners from the losers, the successful and the failures, the acquiring from the acquired, the survivors from the others."

CDR David P. Brown, U.S. Navy, is currently serving as the systems engineering course director for the Advanced Program Management Course at the Defense Systems Management College. He is a member of the International Council On Systems Engineering. Research work for this paper was conducted as a project for INFT 850, Systems Engineering Integration, taught by Andrew Sage at George Mason University, in pursuit of a Ph.D. degree in information technology.

(E-mail address: brown_dave@dsmc.dsm.mil)

References

Enterprise Architecture Project Final Report. (1996). Stanford University.

Farrow, V. (1999, April). *Responding to Change: A Lucent Technologies Program for Growth.* Presentation to PEO/SYSCOM Commanders' Workshop.

Government Accounting Office. (1996, August 26). *Federal downsizing: Better workforce and strategic planning could have made buyouts more effective* (Chapter Report No. GAO/GGD-96-62). Washington, DC: Author.

Industrial automation systems—Requirements for enterprise-reference architectures and methodologies. (1998). http://www.mel.nist.gov/sc5wg1/gera-std/15704fdis.htm, ISO Central Secretariat, Geneva, Switzerland.

Stevenson, D. A. (1995, June). *Business themes and enterprise architecture — conclusions.* http://users.iafrica.com/d/de/denniss/text/busthemx.html, University of Cape Town, Cape Town, South Africa.

Spewak, S. H., with Hill, S. C. (1993). *Enterprise architecture planning: Developing a blueprint for data, applications, and technology.* New York: John Wiley & Sons.

Zachman, J. A. (1997, March). *Enterprise architecture: The issue of the century.* http://www.zifa.com/zifajz01.htm, Database Programming and Design, Zachman International.

CESA: THE COTR EXPERT SYSTEM AID

Dr. Jay Liebowitz

One of the first expert systems developed for the acquisition and procurement and contracting area was built at the Navy Center for Applied Research in Artificial Intelligence at the U.S. Naval Research Laboratory. This case study serves as a key reference in using expert systems in the acquisition area and provides lessons for further advances in this area.

Expert systems are computer programs that act like human experts in a well-defined task of knowledge. They have been applied in diagnosis, classification, interpretation, planning, scheduling, monitoring, and a myriad of other functional tasks. Expert systems are being used to provide estate and tax planning advice, to aid in computer configuration, to assist in medical diagnosis—and in many other applications. They are particularly useful in areas of low-interest, high-utility tasks.

Contracting is one such area. Knowledge of contracting may hold little interest for a physicist, chemist, or computer scientist, but all of them will ultimately be involved in some form of contracting in order to perform his or her job, at least within the U.S. government setting.

At the U.S. Naval Research Laboratory (NRL), an expert system called CESA (COTR [contracting officer technical representative] expert system aid) was developed to provide advice on pre-award areas in contracting. It was built at the NRL's Navy Center for Applied Research in Artificial Intelligence (NCARAI) by the author (a professor at George Washington University at that time), Laura Davis (one of the scientists at the NCARAI), and Virginia Dean (our domain expert with about 27 years of contracting experience).

The COTR is an individual who monitors a contract once it has been awarded, and usually is the same person who assembles the procurement request package that leads to the contract award. The main difficulty in this process, in terms of the COTR's responsibilities, is

the ability to put together a complete and accurate procurement request package. This pre-award area is somewhat complex, because there are a myriad of rules, regulations, and forms with which the COTR must be familiar.

CESA was developed to make the process of putting together the procurement request easier and less time-consuming for the COTR. The acquisition request originator (ARO) is responsible for handling the pre-award phase of a potential contract; and after the contract is awarded, the COTR then is responsible for monitoring the contract. At the NRL, the same person typically serves as both the ARO and the COTR. CESA was designed to help the ARO/COTR by:

- answering questions about the pre-award phase of a contract;
- providing advice about completing selected pre-award forms and showing sample completions; and
- providing information about selected pre-award areas.

In the following sections, the traditional knowledge-engineering life-cycle development steps (Liebowitz, 1999; Cantu-Ortiz and Liebowitz, 1998) will be described as they pertain to CESA.

Problem Selection

Contracts management at NRL responded to a suggestion by a research scientist (and COTR) to contracts management at NRL that expert systems technology might be applied to aid the ARO/COTR in the performance of his or her duties. The NCARAI conducted a feasibility study that identified four possible alternatives for system development (Davis, Liebowitz and Harris, 1988):

- an expert system prototype for procurement request generation and routing;
- an expert system prototype for specific problem-solving activities in relation to contract performance;
- an expert system prototype to supplement conventional ARO/COTR training; and
- an expert system prototype to aid in monitoring the progress of a contract.

These four possibilities were analyzed using the analytic hierarchy process, a methodology developed by Saaty (1980) that assists the decision maker in quantifying subjective judgments. The goal was to decide which expert system prototype would be most feasible. In this analysis, the top-level criteria used to determine the amenability of each alternative to expert system development were: problem characteristics, availability and nature of expertise, and domain personnel. The criteria were weighted via pairwise comparisons and then each alternative was weighted according to pairwise judgments. The final synthesis step then took into account the weighted criteria and weighted the order of alternatives to rank the alternatives.

The results (Liebowitz, Davis, and Harris, 1989) indicated that the two areas of COTR problem-solving activities relating to contract performance and procurement

request generation appeared particularly amenable to expert system development. Numerous discussions with a variety of individuals, particularly our contracts expert who had about 27 years of contracting experience, led to the decision to concentrate on the pre-award phase (i.e., procurement request generation) rather than the post-award phase (i.e., contract progress and performance) for the development of the expert system prototype.

Of paramount importance to the ARO/COTR is speed in the contracting process. Experience at NRL has shown that contracting specialists and officers frequently receive incomplete or inaccurate procurement request packages that need to be returned to the ARO for additions or corrections before processing, thereby delaying the procurement process. Thus the highly structured and specific nature of the contracting pre-award phase, coupled with the strong need for aid in this area, positioned procurement request generation as a high-interest, high-payoff domain for expert systems development.

Prototype Development

The development of CESA followed the rapid prototyping, knowledge engineering process of knowledge acquisition, knowledge representation, knowledge encoding, and knowledge testing and evaluation (Liebowitz, Davis, and Harris, 1989). The "build-a-little, test-a-little" evolutionary approach resulted in an initial, approximately 150-rule proof-of-concept version of CESA within a few months (Liebowitz, Davis, and Harris, 1990). Following a year of development, CESA had 246 rules in its knowledge base.

Knowledge Acquisition

Knowledge for CESA was acquired through two major sources. The first was through perusal of many NRL instructions and manuals that address the pre-award contract phase. The second was through extensive interactions with a contracts expert. To prepare itself to deal more effectively with both sources, the knowledge engineering team also attended several formal ARO and COTR training (lecture) courses. The project was fortunate in having the services of a highly experienced, enthusiastic contracts expert who felt there was a great need for developing a system such as CESA to assist ARO/COTRs at NRL. As a retired annuitant, she was also excited that her expertise would be "preserved" and used to help others at the laboratory.

"Following a year of development, CESA had 246 rules in its knowledge base."

In acquiring knowledge from the expert, various interviewing methods were used. Structured interviews were effective because once the major pre-award areas were mapped out, the knowledge engineering team could acquire knowledge from the expert systematically in each of these areas, one at a time. For example, after the first two interviews with the expert, it was determined that the pre-award phase could be decomposed into the following major areas of concern:

- Adequacy of the procurement request (PR) package (this area is subdivided

into five parts: what is needed in the package, justification and approval [J&A] if the requirement to be specified is sole source, statement of work [SOW], evaluation procedures, and synopsis procedures);

- routing of the PR or of the procurement planning document;
- use of the procurement planning document; and
- use of the ADP procurement checklist.

The technique of using "constrained information tasks" (i.e., having the experts reason through their decision making process within a limited amount of time) forced experts to think within a short period of time and helped identify for the knowledge engineers the salient heuristics involved. Employing "limited information" during parts of the interview required experts to determine what was important in terms of material used and information omitted. Also quite productive was the use of scenarios, whereby experts would "think aloud" during the process of solving sample cases posed by the knowledge engineers.

Rule Number 68

IF:

Your questions involve the pre-award phase

and you want to know what is needed in a PR package,

and your procurement is a major procurement costing $25,000 or more,

and appropriate type of contract is firm fixed-price (FFP),

and procurement request is for capital equipment OR sponsor-funded equipment,

and your procurement request deals with acquisition of commercially available hardware, software, or materials where the vendor can quote a price that won't change during the life of the contract, and can deliver at that price (vendor assumes risk),

THEN:

No SOW is needed. However, you must include product functional or performance specifications or standards of performance (salient features—brand name or equal is applicable), described in terms of mandatory minimum requirements/specifications. Confidence = 10/10

Knowledge Representation

Throughout the knowledge acquisition sessions with an expert, it was apparent that the expert's knowledge fell naturally into condition-action or if-then rules. The appropriateness of this format for CESA's knowledge base was further strengthened by reviewing contracting documentation, in which if-then clauses are a frequent construct. Thus the knowledge representation mechanism selected for CESA was production rules, with the average rule containing five to six antecedents (the "if" part) and two to three consequents (the "then" part). An example rule from CESA's knowledge base is in the box on page XX (NRL Instruction, 1988).

Knowledge Encoding

To help speed the process of demonstrating the feasibility of an expert system prototype to aid the ARO/COTR to a sponsor unfamiliar with the technology, CESA was developed using an expert system shell (which allows the expert systems developer to concentrate on the construction of the set of facts and rules of thumb [i.e., knowledge base] for this application). Requirements of a shell for this application included:

- ability to handle backward chaining (i.e., goal-directed reasoning from conclusions to facts), and preferably forward chaining (i.e., data-driven reasoning from facts to conclusions) as well;
- provision for production rules;
- accommodation of free-text comments;
- management of uncertainty in rules;
- application of easy-to-use text editor;
- provision for linkages to external programs or data; and
- availability on IBM PC or PC-compatible computers.

Based on these considerations (as well as a relatively low price and the availability of an unlimited copy, run-time license for use within NRL) the shell Exsys Professional (Multilogic, 1988) was acquired for the development of CESA. (Exsys is now called Resolver/Exsys Developer and can be run over the web via NetRunner/ Exsys Web Runtime, both products by Multilogic, Inc.)

Encoding the knowledge base for CESA using Exsys was an iterative process. After acquiring and representing the knowledge for a particular pre-award area, it was subsequently encoded into the system. With prototypical cases quickly encoded into CESA, the expert could see some tangible results occurring from the knowledge acquisition sessions, and could also more easily identify omissions in the knowledge or the application of incorrect knowledge. Through observing the chaining taking place in CESA, the expert was able to confirm that proper conclusions were being reached from the combinations of input provided. When weaknesses in the knowledge base were identified, the

"Throughout the knowledge acquisition sessions with the expert, it was apparent that the expert's knowledge fell naturally into condition-action or if-then rules."

knowledge was reacquired, represented, and encoded into CESA.

Knowledge Testing and System Evaluation

Knowledge testing (including both verification and validation) and system evaluation have been performed iteratively for each version of CESA (Davis and Liebowitz, 1990; Prerau, 1989). Verification has involved exhaustively checking all possible combinations of responses in CESA for logical consistency, an increasingly time-consuming task as the number of rules grew with each version (CESA currently has 246 rules).

Validation was performed in various ways throughout system development to test the quality of CESA's advice. One method used was backcasting, which involves historical test cases being used to compare CESA's recommendations with actual, documented results. In addition to those that fell squarely within the scope of CESA, cases were selected to push CESA's boundaries to examine its robustness; others were chosen to determine exceptions to CESA's rules. A second domain expert also developed and then ran sample sessions with the prototype and critiqued its advice.

"Validation was performed in various ways throughout system development to test the quality of CESA's advice."

A preliminary evaluation was also conducted by soliciting the comments of several COTRs on the human factors aspects of CESA after they had tried the system. Although the shell limited the flexibility of display of questions and advice, the users made helpful suggestions that led to the rewording of questions, inclusion of free-text explanations, and definition of terms at critical points, and reworking of the presentation of conclusions. This aspect of system refinement is especially important since contracting terminology, second nature to the domain expert, may be unfamiliar to many within the CESA user community.

Field testing and evaluation has proceeded in two stages. Initially, a small group of five test users was selected using the following guidelines:

- A range of levels of user contracting knowledge, from naïve through experienced, is obtained.
- The affiliations of the users represent a sample of the variety of procurement request actions found at NRL.
- Users are motivated to participate in the test group.
- Users have access to the necessary computer hardware.

Test users in the group were briefed and trained, and were given evaluation questionnaires to complete at the end of each week of the four-week initial test period. The questionnaires (a total of 11 per user) were designed to require each test user to eventually try each contracting area within CESA. This imposed some structure on the testing and evaluation process, but left room for additional exploration and corresponding comments according to each user's inclination and preferences. In general, the test users were quite pleased

with the accuracy of advice provided by CESA and impressed by its ease of use. They felt the system would save time in preparing complete procurement request packages, with particular benefit in training new ARO/COTRs and in double-checking and updating more experienced COTRs' knowledge.

The second stage of field testing and evaluation involved a larger group: more than 30 test users, encompassing all of NRL's research and support divisions to provide a wider spectrum of the NRL ARO/COTR community. They used CESA over a two-month period at the end of the fiscal year, a peak time for procurement request generation. The test users in this group were also asked to complete evaluation questionnaires, from which the following results were calculated (Table 1).

Overall, the test users reinforced the quite favorable response to CESA expressed by the earlier test group, and also offered some useful suggestions that have now been incorporated into the current version of the system.

Maintenance

Maintenance is a critical activity in any expert system's development life cycle (Turban and Liebowitz, 1992). The issue of maintenance is extremely important to the utility and success of CESA, because contracts rules and regulations change frequently and CESA is of little value without current, up-to-date information. From the beginning, maintenance has been an important consideration in the design and implementation of CESA.

Several factors directly contribute to easing its maintenance. First, CESA's knowledge base was structured in a modular fashion, so that rules are grouped by

Table 1. Second-Stage Evaluation of CESA

Criteria	Average Score
Quality of the advice or conclusions reached	9–10
Line of questioning	8.56–10
Clarity and completeness of questions and free-text comments	7.32–10
Conclusions of CESA	8.69–10
Explanations and instructions	7.93–10
Response time and hardware	8.38–10
Graphics	8.38–10
Utility:	
How pleased were you overall with CESA?	8–10
How useful do you find CESA as a training tool to supplement the ARO/COTR courses?	8.78–10

pre-award area with little, if any, "interlinking" between such areas. Additionally, sufficient redundancy was introduced to minimize any complex rule interactions. Second, an advantage to using an expert system shell such as Exsys for system implementation is that it has straightforward, relatively easy-to-use knowledge base editing facilities that do not require a computer expert. Finally, an infrastructure was developed within contracts management at NRL, where two contracts personnel (with contracting expertise and some personal computer experience) were gradually assuming the maintenance of CESA as part of their official responsibilities.

"To initiate the transition and build contract management's confidence in maintaining CESA, a seven-week training program was conducted for two contracts personnel and also a program analyst at NCARAI."

Unfortunately, however, this responsibility for maintaining CESA was never officially documented as part of their job descriptions and was not included as part of their annual job performance review. As a result of this major oversight, the "maintainers" would update CESA if they had a chance. Since there was a flurry of activity in the contracts area and since these individuals weren't being evaluated on how well CESA was being maintained, CESA's accuracy began to degrade over the next four months as new rules and regulations were made and were not incorporated into CESA's knowledge base. To ensure successful transitioning, NCARAI had planned to provide oversight and serve as a consultant to contracts management in the maintenance of CESA.

To initiate the transition and build contract management's confidence in maintaining CESA, a seven-week training program was conducted for two contracts personnel and also a program analyst at NCARAI. Each training session met for approximately one hour, once a week, within an incremental, structured program plan for the seven-week period. The hands-on training sessions progressed from an overview of expert systems and CESA's development through learning how to use Exsys Professional to learning how to use and maintain CESA. The trainees were eased into the process of maintaining the expert system by first learning how to use Exsys; then understanding how CESA's knowledge base is structured; and finally learning how to move, edit, add, delete, and debug CESA's rules. Take-back-to-the-office exercises were assigned at the close of each training session to reinforce the ideas just covered and further increase familiarity with Exsys and CESA.

As part of the training, the group also observed how the knowledge engineers went about debugging and maintaining CESA. After the formal training program was completed, the trainees were encouraged to continue to familiarize themselves with CESA and Exsys as we eased into the transition process.

Lessons Learned

Several lessons contributed to the initial success of CESA. First, there was an overwhelming need for such support for

the COTR community. At NRL, the COTR community is extremely diverse. ARO/COTRs range in experience from the novice, trained but yet to serve on his or her first contract, to those with years of experience on a variety of contracts. Most technical personnel find contract terminology quite unfamiliar, and the more specific ARO/COTR functions and procedures, along with the terms, can fade from memory as time between contract assignments lengthens. Also, as theory is put into practice on an ARO/COTR assignment, understanding at a conceptual level can give way to uncertainty and confusion at the practical level. Since contracts management is often as overburdened as the technical personnel they support, their inaccessibility can further frustrate the ARO/COTR seeking answers to his or her inevitable questions. Indeed, it was a member of the COTR community who first suggested the application of expert system technology to aid the ARO/COTR.

A second lesson learned from the development of CESA was that hypertext (Shafer, 1988; Conklin, 1987; Fiderio, 1988; Anacker, 1988; Rada, Dunne and Barlow, 1990; Arnett, 1989; Patton, 1988; and Chian, 1990) proved to be a very useful capability to furthering support of CESA by the users. By simply hitting a function key, users could obtain advice on how to complete selected pre-award forms or could view examples of completed forms, all through hypertext screens. The hypertext capability allowed the user to easily obtain detailed information on how to complete procurement request forms.

In this manner, the merging of expert systems technology with hypertext was quite successful. CESA, through its expert systems technology, would as part of its advice tell the user what forms he or she would need to use for assembling an adequate procurement request package. Through the hypertext addition, CESA would not only tell the user what forms were needed but also would allow the user to complete and print out some of those necessary forms.

Another major lesson learned was that the combination of a supportive upper-management, dedicated and enthusiastic expert, and early and continued user involvement helped ensure a successful development of CESA. As we deployed CESA, the CESA team was still learning more about how to properly "institutionalize" (Liebowitz, 1991) CESA within NRL so that maintenance of CESA was easily facilitated. As these issues became solidified, the hope was that CESA would serve as a very useful tool to aiding the 2,000 COTRs within NRL.

"The last and perhaps most important lesson learned is the need for building a supportive culture...."

The last and perhaps most important lesson learned is the need for building a supportive culture (Liebowitz, 1998; Liebowitz and Beckman, 1998; Liebowitz, 1999) as part of the expert system's institutionalization process and providing the right mechanisms and incentives to keep the expert system alive and breathing. The fundamental error of not evaluating how well CESA was being maintained as part of the maintainer's annual job performance review provided no incentive to properly keep CESA's knowledge base up-to-date. This factor,

coupled with the fact that the main project champion (i.e., the head of the contracts division) moved to another assignment in the Pentagon, killed the strong support and continued enthusiasm for the project. As a result, CESA was a technical success but a technology transfer failure.

Implications for the Acquisition Researcher

CESA is now being developed in the Laboratory for Knowledge Management at the University of Maryland–Baltimore County into a web-based, intelligent multiagent system using a brokered agency architecture, via an External Acquisition Research Program grant. This architecture involves having five specialty agents (synopsis agent, forms agent, evaluation agent, justification and approval agent, and type of contract desired agent) which are integrated with a user agent. Through the interaction with the user agent, the user can ask general questions about the pre-award phase of a contract, and the user agent will send the question to the specialty agents for a response. We have used AgentBuilder by Reticular Systems as a tool to assist us in the development of these agents, based upon the CESA knowledge base. We are currently looking into incorporating learning within the multiagent system so that the specialty agents can learn from each other.

The CESA case study offers the acquisition researcher several important lessons. First, people and culture are probably more important critical success factors than the technology itself. Thinking about implementation concerns should be done in the planning stage in order to reduce resistance to change when finally introducing a new system into the organization. Second, expert systems are a valuable business solution and they seem to be reappearing now in the emerging trend of "knowledge management." Third, with web-based and intranet technologies, intelligent agent approaches should be considered for development and use in the acquisition domain. This direction is where some promising research can result in the acquisition community.

Jay Liebowitz, Ph.D., is the Robert W. Deutsch Distinguished Professor of Information Systems and the University of Maryland-Baltimore County. Previously, he was professor of management science at The George Washington University and the chair of artificial intelligence at the U.S. Army War College. He is the editor-in-chief of *Expert Systems With Applications: An International Journal* (Elsevier), and is the founder and chair of The World Congress on Expert Systems.
(E-mail address: liebowit@umbc.edu)

REFERENCES

Anacker, P. (1988, November-December). Thinking tools. *PC AI Magazine.*

Arnett, N. (1989, August). Computing faces dawn of a new age. *Computer Graphics World.*

Cantu-Ortiz, F., & Liebowitz, J. (Eds.). (1998, March). *The 4th world congress on expert systems proceedings.* New York: Cognizant Communication Corp.

Chian, D. (1990) *CESA and hypertext* (unpublished report). Washington, DC: Navy Center for Applied Research in Artificial Intelligence, Naval Research Laboratory.

Conklin, J. (1987, September). Hypertext: An introduction and survey. *IEEE Computer, 20*(9).

Davis, L., & Liebowitz, J. (1990, April). Testing and evaluation of expert system prototype: A case study. *Information Age, 12*(2).

Davis, L. C., Liebowitz, J., & Harris, W. F. (1998, January). *Feasibility of developing an expert system to aid the COTR in contract administration* (NRL Technical Memorandum). Washington, DC: Navy Center for Applied Research in Artificial Intelligence, Naval Research Laboratory.

Multilogic Inc. (1988). *Exsys: Expert system development package.* Albuquerque, NM: Author.

Fiderio, J. (1998, October). Hypertext: A grand vision. *Byte.*

Liebowitz, J. (1991). *Institutionalizing expert systems: A handbook for managers.* Englewood Cliffs, NJ: Prentice Hall.

Liebowitz, J. (ed.). (1998). *The handbook on applied expert systems.* Boca Raton, FL: CRC Press.

Liebowitz, J. (ed.). (1999a). *The knowledge management handbook.* Boca Raton, FL: CRC Press.

Liebowitz, J. (ed.). (1999b). *Expert systems with applications: An international journal.* London: Elsevier.

Liebowitz, J., & Beckman, T. (1998). *Knowledge organizations: What every manager should know.* Boca Raton, FL: St. Lucie/CRC Press.

Liebowitz, J., Davis, L .C., & Harris, W. F. (1989). Using expert systems to help the contracting officer technical representative: A feasibility study and selection methodology. In *Educational technology.* Englewood Cliffs, NJ: Educational Technology Publications.

Liebowitz, J., Davis, L .C., & Harris, W. F. (1990). CESA: An expert system prototype for aiding U.S. Department of Defense research contracting. In J. Liebowitz (Ed.), *Expert systems for business and management.* Englewood Cliffs, NJ: Prentice Hall.

Liebowitz, J., & DeSalvo, D. A. (Eds.). (1989). *Structuring expert systems: Domain, design, and development.* New York: Yourdon.

NRL Instruction (1988, April 19). Rule 4205.3A. Washington, DC: Author.

Patton, C. (1988, October 10). Professionals adopting pint-sized expert systems. *Computerworld.*

Prerau, D. (1989). *Developing and managing expert systems.* Reading, MA: Addison Wesley.

Rada, R., Dunne, P., & Barlow, J. (1990). EXPERTEXT: From semantic nets to logic Petri nets. *Expert Systems with Applications: An International Journal, 1*(1).

Saaty, T. L. (1980). *The analytic hierarchy process.* New York: McGraw-Hill.

Shafer, D. (1988, May-June). Hypermedia and expert systems: A marriage made in hyper heaven. *Hyperage.*

Turban, E., & Liebowitz, J. (Eds.) (1992). *Managing expert systems.* Harrisburg, PA: Idea Group Publishing.

PRIVATE SECTOR DOWNSIZING: *IMPLICATIONS FOR DOD*

Michael L. Marshall and J. Eric Hazell

The Department of Defense surges forward with plans to increase efficiency by downsizing its in-house laboratories. Corporate America's adventure with such policies during the past decade, however, has left it with strong second thoughts (as well as low employee morale, high turnover, stagnant profits, and little increase in productivity).

Since the end of the Cold War in the late 1980s, the Department of Defense (DoD) has been continuously engaged in reducing workforce levels, both military and civilian. These drawdowns have affected every defense agency and component, including the DoD's in-house laboratories. Workforce reductions at many of these laboratories are expected to exceed 40 percent by the end of this decade (as measured from a 1991 baseline).

Still, there are many voices, both within and outside of DoD, calling for most of the remaining work in these laboratories to be contracted out to the private sector. Proponents of this outsourcing strategy imagine that the remaining in-house workforce can be drawn down to some "irreducible core" number of employees —seemingly, the smaller the better—who would only engage in inherently governmental work. Implicit in this strategy is the assumption that the size of the irreducible core can be determined and in fact realized. Is this a valid assumption? Or, will the downsizing journey undertaken to reach this irreducible core destroy the very thing that is claimed should be preserved?

The private sector has now been engaged in downsizing for many years. As a result, a large body of literature dealing with lessons learned from corporate downsizing has accumulated. Tellingly, this literature demonstrates the many

negative effects of downsizing—its adverse impact on employee loyalty, the loss of invaluable corporate memory, and the resulting high cost of employee turnover. A study of this private sector experience could do much to inform decision makers who believe significant additional workforce reductions in the DoD's in-house laboratories can be sustained without doing irreparable harm to their ability to perform even a set of core functions.

In-House Laboratories—Evolution and Enduring Need

The present community of DoD in-house laboratories has a rich history, with roots stretching back for more than 150 years. Indeed, some of the Navy component activities that make up this community had their roots in legislation passed by Congress in 1841, which first established the Navy bureau system. Over time, the component activities of this community have evolved from small, specialized, laboratories focused on a particular component (e.g., fuse) or weapon (e.g., gun, torpedo) to warfare-oriented, Research, Development, Test and Evaluation (RDT&E), technical centers (Carlisle, 1996; Carlisle, 1997).

Over the past 40 years, many authoritative statements regarding the importance of maintaining an in-house laboratory capability in the DoD have been made (Steelman, 1947; President's Science Advisory Committee, 1958; Bell, 1962; Sheingold, 1966; Government Accounting Office, 1981; Messere, 1983; and Langenbeck, 1982). While these statements often reflected different emphasis, they all held the common assumption that there is an enduring need for such laboratories.

For example, in October 1961, during the height of the Cold War, then-Secretary of Defense Robert McNamara declared that "in-house laboratories shall be used as the primary means of carrying out Defense Department Research and Development programs." Some 15 years later, John Allen, then Deputy Director of Defense Research and Engineering (Research and Advanced Technology), stated in a Blue Ribbon panel study that although a lot of innovation in the Department's technology base came from contractors,

> No way has been found to preserve the combination of current technical expertise and long-term corporate memory other than setting up an organization wherein individuals can maintain a lasting and close association with their Service while staying involved in technology; in short, an in-house laboratory.

In its 1994 response to a laboratory review directive issued by President Bill Clinton, DoD stated that its laboratories are "integral components of the military departments' acquisition and combat support infrastructure." Furthermore, the response noted:

> The essential barrier to outsourcing, and thus the principal competitive advantage of the DoD labs, is their mission motivation in total congruence with the customer, their identification with

> and closeness to the warfighter of the U.S. Combatant commands... Only in-house, dedicated organizations truly share the commitment of their parent commands.

Such authoritative comments verify the continuing importance of in-house defense laboratories—there is little real debate over whether such labs are needed. But they provide little guidance on sizing this community. How many labs are needed, and how large or small should they be? How should their work be focused? The prevailing wisdom today is that they should be no larger than some irreducible core, and they should only do those things reserved exclusively to the government. This outlook derives from a few major sources, a major one being the downsizing efforts of corporations over the past couple of decades.

Drivers for Private Sector Downsizing

Corporate downsizing has been a trend for almost a quarter century. It has been driven by a number of pressures. Some of these pressures have varied over time (e.g., the effect of a recession). Others have exerted a more or less steady influence.

The first of these pressures was leveraged buyouts (LBOs). In the late 1970s and into the early 1980s, many companies became strapped with huge debt as the result of LBOs. To ease cash-flow concerns, many of these companies sought relief by cutting costs, mainly by workforce reductions.

A second pressure was recession. In the latter 1980s and into the 1990s, worldwide recession led to cutting costs and restructuring. As demand fell, companies found themselves with excess capacity. They reacted by cutting infrastructure and cutting people.

Moreover, this period witnessed unparalleled growth in global competition. Again, to survive in this environment, many companies resorted to cost-cutting measures. Some moved operations offshore to take advantage of cheap labor. Others made business process improvements and introduced more efficient plant equipment. In both cases the result was a lower demand for American labor, which led to downsizing.

"Corporate downsizing has been a trend for almost a quarter century."

Another factor has also fed the downsizing frenzy—the rush to increase bottom-line profitability. Since the early 1990s many corporate chief executive officers (CEOs) have pushed hard to increase bottom-line profitability, in part to drive up share prices. Church et al. (1996) states that attempting to reduce costs by reducing personnel tempts executives, because the only ways to increase profits are by increasing revenues or decreasing costs. Most agree that future costs are easier to predict than future revenues, and as "human resources represent costs...it seems logical to reduce those costs through decreasing the number of employees." The primary questions in many boardrooms are: What is the irreducible core number, and how do we get to the irreducible core number of employees we need to operate?

Off with Their Heads

As indicated, to raise profits a company can either increase revenues or cut costs. Labor costs loom large on corporate balance sheets—about 50 percent of operating costs in a service company—so naturally, attacking the payroll is the solution *du jour* for most CEOs (Coolidge, 1998). Coolidge notes that the focus on cutting headcount may be headstrong. Nevertheless, history has shown that reducing "headcount" has been the preferred method of cutting costs, largely because it seems to be the most expedient method.

While some literature indicates that downsizing can benefit an organization, at least in the short term, there is growing evidence that suggests downsizing is dysfunctional for both organizations and their employees. The costs of this strategy are enormous and usually underestimated. In fact, they often more than offset any anticipated benefits.

"Sometimes, downsizing too massive or frequent can put a company into a death spiral...."

Indeed, massive downsizing frequently generates more problems than it solves, and almost never achieves its original financial objectives (Borque, 1995; Gosselin, 1994; Dupuis, Boucher and Clavel, 1996). It frequently causes the best and brightest employees to leave the organization. And these are the very employees the organization needs to survive. The costs of replacing them with new employees are enormous for an organization that has lost its best people and, with them, their special know-how and expertise (Margulis, 1994; Dupuis, Boucher and Clavel, 1996).

Sometimes, downsizing too massive or frequent can put a company into a death spiral (Dupuis, Boucher and Clavel, 1996). This happens when the first round of downsizing does not produce the requisite result in savings, necessitating still more cuts. In the interim, those who remain become demoralized, overworked, and less productive. Revenue then falls and the company has to cut again.

Mark Mone (1997), citing a number of other studies, questions the efficacy of downsizing as a cost-cutting strategy. This literature points out that large-scale sample research matching firms by extent of decline, industry, size, and age, demonstrates that organizations that downsize have no better return on investment, sales gains or other objectively measured bottom-line outcomes than those organizations not downsizing.

Professor Kim Cameron, who has studied private sector downsizing for more than 20 years, comments (1997):

> [Downsizing] is most often implemented as a grenade strategy... you throw a grenade into a company and it explodes, eliminating the positions of a certain number of people. The problem is you have no way of telling precisely who is going to be affected. In the end, a corporation almost always loses corporate memory and company energy.

Research by Cameron and others confirms that whereas in the 1980s and early 1990s, downsizing almost always focused on head count, today CEOs are beginning

to consider the bigger picture of changing the culture of the organization. They recognize that merely cutting headcount, without attending to the fundamental problems causing inefficiency and lack of competitiveness, will mean the same problems will persist even after downsizing. Commenting on this, Cameron notes that "Companies are now realizing that they have to redesign to avoid the problem of overloading fewer workers with the same amount of work using the same organizational arrangements." What follows is a more in-depth analysis of the problems with downsizing.

Negative Effects of Cutting Headcount

First, downsizing often adversely affects employees remaining at the organization. Sharma (1996) provides a view increasingly held by researchers:

> Downsizing sounds good on paper, but it can cost a company a lot of money. People trained in important techniques and skills over the years expect their heads to hit the chopping block next, and get out as soon as they can. The company is left with the second best. One layoff can ruin morale for the next few years, and the cost of rebuilding can eat up the dollars saved by the original "cure" for the company's financial illness, and more.

Mone (1997), citing a great deal of the relevant literature, points out that organizational downsizing can have a variety of dysfunctional consequences on surviving employees. Indeed, the litany of negative effects these researchers have noted is almost mind-numbing: decreases in morale, trust, concentration, satisfaction, commitment, and productivity; increases in guilt, stress, workloads, absences, tardiness, theft, cynicism, and opportunism. Mone (1994) further indicates that increased turnover and intentions to leave may also follow downsizing.

Focusing on a specific instance listed above, we can see that the psychological effects of downsizing can infect the health of the surviving employees. For example, one study (La Voie, 1997) confirmed a relation between downsizing and subsequent employee absenteeism because of ill health. The study found that the extent to which employees' health was affected depended on the degree of downsizing. Specifically, it found that the rate of long-term sick leave (more than three days) was 1.9 to 6.9 times greater after major downsizing than after minor downsizing. Overall, long-term sick leave increased by 16 to 31 percent during this period of downsizing. Consequences of such trends on productivity are obvious.

"First, downsizing often adversely affects employees remaining at the organization."

This effect is also the subject of a recent book by David Noer (1993). Noer believes that this "survivor sickness" can harm the organization's health, as survivors continue to be "angry, anxious, and depressed for years after the layoffs." He advocates serious intervention to deal with this sickness, to avoid emotional distress and productivity paralysis (Chaudron, 1994).

Finally, Kirsten Haggis has tried to make sense of this dizzying array of ill effects, classifying them into three clusters. These include fear (uncertainty, insecurity, "Why me?"), frustration (resentment, anger, blaming), and uneasiness (betrayal, distrust, disillusionment). If such emotions are not recognized and carefully dealt with, she asserts, they can in many ways cripple an organization.

"The possibility exists for cyber attacks of every type, and the results can be catastrophic."

Collectively, this research argues that the survivors—despite still having jobs—are primarily affected negatively by the downsizing experience. Consequently of course, their organization suffers.

The Emergence of the "Volunteer Workforce"

One major casualty of the downsizing trend, as might be expected from the above discussion, has been an erosion of worker loyalty to the organization. Decreased commitment has, in turn, resulted in increased employee turnover, with all of its associated costs. As a result, many businesses now consider keeping skilled employees a major problem, one which, if solved, can lead to greater competitive advantage.

The erosion of employee commitment has been well documented. Nearly 4 in 10 firms recently surveyed by William M. Mercer Inc. reported an upswing in turnover in the past 3 years. (Gemignani, 1998) Another study found that nationally, the average annual employee turnover rate for all companies is 12 percent (Bureau of National Affairs, 1998). In the United States there is a 30 percent turnover in all front-line jobs. A 1996 Wisconsin study found that "75 percent of the demand for new employees is simply to replace workers who have left a company." (Positive Directions, Inc., 1998; Pinkovitz, et al., 1996–97).

Perhaps this decline in commitment has been demonstrated most forcefully in a recent study by AON Consulting. Entitled "America@Work," it concludes that employee loyalty is a thing of the past. The study found that today's workers face more stress on the job, want more time for their personal lives, and will switch jobs for relatively small increases in pay. In fact, more than 25 percent of those surveyed said they would "jump ship" for a pay raise of 10 percent or less, while more than 50 percent said they would do so for a raise of 20 percent or less. As the authors note, "Today's workers are more educated, entrepreneurial, and independent than ever, and are more discerning in choosing where to work. Particularly in this tight labor market, it is getting much tougher for businesses to hang on to their best and brightest employees." (Stum, 1998)

Attracting and retaining employees in high-technology businesses, including defense, is a particularly troublesome issue. Part of the difficulty lies in recent employment trends in such areas. Luker and Lyons (1997), using data covering the period 1988–1996, found that the industrial composition of employment in research and development (R&D) -intensive, high-technology industries is shifting dramatically toward services industries,

as employment in R&D-intensive, defense-dependent manufacturing industries declines, and employment in civilian high-tech manufacturing remains essentially static.

In fact, their data demonstrate that R&D-intensive services accounted for all of the net increase in employment in the R&D-intensive sector since 1988, and grew more rapidly than did employment in the services division as a whole. In essence, more and more R&D workers in the United States are moving into the service sector where job turnover is particularly volatile. The authors comment:

> The closer a firm is to the technological frontier...the stronger will be its demand for high-tech workers...And no matter how many scientists and engineers there are, they are always in short supply. Job creation, job destruction, and...job switching... occur among the most technologically innovative firms, [and worker] instability, of course, can result in dynamic losses of knowledge...In order to attract and keep R&D talent, then, firms must cultivate well-articulated internal labor markets for scientists, engineers, and other classes of skilled employees, providing high wages and benefits, and emphasize participation in state-of-the-art projects.

The defense industry, which has in the past been so dependent on manufacturing, may also have difficulty keeping its R&D workers from moving to the lucrative non-defense service sector. Anecdotal evidence suggests recruitment is already a growing problem in the defense industrial sector, with some firms now offering bonuses of several thousand dollars to employees who bring in new recruits.

The problem could be even more acute for high-tech defense and manufacturing industries with a high proportion of information technology (IT) workers—for example electrical engineers, computer scientists, computer engineers, systems analysts, and computer programmers—because there is a growing shortage of such workers in the United States. The Department of Commerce (1997) has documented the extent of this shortage. As a result, salaries and benefits packages in the non-defense commercial IT sector are soaring as companies target defense workers, both in government and industry, as a prime source of new high-tech employees. Recently in *Government Executive* Magazine, Richard Lardner (1998) illustrates this trend in an article dealing with the ongoing brain drain at the National Security Agency, where mathematicians and IT workers are being lured away to the non-defense commercial sector by firms such as Price Waterhouse.

"The volunteer workforce, in sum, has fundamentally changed the kinds of issues and problems for today's corporate executives and managers."

The volunteer workforce, in sum, has fundamentally changed the kinds of issues and problems for today's corporate executives and managers. As Nancy Lyons points out, the best employees now "elect to work where they do simply because it's

the kind of place they like to show up at every day." They want challenging and exciting work, and they are in demand. This is why in a recent survey of 1,443 members of TEC (an international organization of CEOs), most cited hiring, training, and keeping employees as the major problem of managers today. There is no sign that this is changing.

Loss of Corporate Memory

Downsizing has had other dire consequences, one of the most important of which is loss of corporate memory. What exactly is corporate memory? Most individuals in an organization, especially the high performers, are storehouses of specialized knowledge. Most are also repositories of organizational folklore and oral tradition which, surprisingly, are essential to the smooth and efficient working of an organization. The knowledge and tradition includes experience in specific projects, networks with clients and contacts, familiarity with company culture, and awareness of an organization's informal relationships and decision-making processes. Collectively, this information is referred to as corporate memory.

"Downsizing has had other dire consequences, one of the most important of which is loss of corporate memory."

Any time people leave, whether voluntarily or involuntarily, they take with them some of this knowledge and lore. When the separation is voluntary, there is at least some opportunity to pass along the more important information to a successor. When the separation is involuntary (e.g., as a result of downsizing), there is a loss of corporate memory (van de Vliet, 1997).

The complex knowledge that departing employees take with them might include the individual's experience with particular projects. Loss of this knowledge can be both dangerous and expensive. Studies at Warwick University in England have shown that many companies reproduce their blunders on a regular basis. The management consultants McKinsey have concluded that many waste time and resources resolving problems that have previously been unraveled in the company. Reinventing the wheel is thus a much more common drain of corporate resources and creativity than most managers imagine. Moreover, as Arnold Kransdorff of Pencorp, the London-based business historians, has pointed out, the dangers of corporate memory loss are particularly acute in an era when downsizing and re-engineering have shortened job tenure to an average 6 years, against the backdrop of an eight-year trade cycle (van de Vliet, 1995).

Corporate amnesia can also be the result of the trend toward outsourcing, according to Margaret Graham, founding partner of the Winthrop Group in Cambridge, MA, one of the leading corporate memory and business history consultants in the United States. She notes that companies intent on reducing their capital base or handing off a problem by outsourcing a function forget the importance of "local knowledge, specific to the company," with serious consequences for productivity. (van de Vlient, 1995).

A number of analysts have also shown the connection between downsizing and

loss of corporate memory ("Corporate Amnesia," 1996). For example, Alan Downs, author of "Corporate Executions: The Ugly Truth About Layoffs—How Corporate Greed is Shattering Lives Companies and Communities," relates a telling anecdote. Downs points out that between 1985 and 1995, Apple laid off about 6,000 people, while at the same time increasing overall headcount each year. Commenting on this, he writes:

> This creates a churning environment of fear and confusion... Having worked at Apple, I know every time they've conducted one of these layoffs, there has been mass confusion; everyone is grasping for their piece of the pie. There's a lot of time lost. One result is that the company lost its competitive edge, failing to develop a new breakthrough product during this entire period.

With each layoff comes a loss of corporate memory, and with each loss of corporate memory comes a loss of productivity and competitiveness. "It's the knowledge, nuances and intuition we bring to day-to-day decision making," says James Challenger, president of Challenger, Gray & Christmas in Northbrook, IL. "A little bit of this invaluable corporate memory disappears each time an individual is laid off ("Losing Corporate Memory," 1996).

Some researchers consider corporate memory a major asset and element of the company's overall intellectual capital. Annie Brooking (1999) writes: "Companies are typically well versed in assessing and valuing tangible assets, such as buildings, machinery, cash and so forth, but such measures do not include the value of the workforce, their knowledge, the way they use computer systems and so on."

Corporate Memory in an R&D Organization

Corporate memory is vitally important to an organization, such as a laboratory, heavily involved with R&D. How innovation occurs in such organizations is of great interest to many, and has been studied extensively. Carlisle (1997) provides a bibliographic guide to some of this literature.

It is becoming clear that much of the innovation depends on informal networks in the organization, networks that until recently have been underappreciated. For one, they enable the collaboration key to innovation. Kreiner and Schultz (1993) have studied informal networks in R&D organizations. Noting the importance of such networks, they point out that "accounts of informal ways of collaborating are dramatically under-represented in the literature, and even then, are often only acknowledged in passing." Examples they cite include "skunkworks" (Quinn, 1985; Peters, 1988), "bootleg research" (Burgelman and Sayles, 1986), and similar concepts that allude to informal patterns within the research lab.

"It is becoming clear that much of the innovation depends on informal networks in the organization, networks that until recently have been underappreciated"

Other researchers reach the same conclusions. Ryne and Teargarden (1997), considering innovation in technical organizations, argue that three critical variables underpin the value-added creation process: skilled human assets; skilled senior leadership, and adequate resources. If any one of the three is absent, value-added creation is unlikely. Competitive organizations use a strong culture to bond these three variables in ways that cultivate core competencies and capabilities. In this analysis, attracting and retaining these skilled technical employees is a crucial technology-based competitive strategy. Indeed, "the ability of the firm to use science and technology to provide value-added products and services is a critical core competence which can yield competitive advantage for firms pursuing technology-based competitive strategies."

"Although it negatively affects remaining workers, erodes loyalty, and weakens corporate memory, all these are only parts of the major problem with downsizing: It costs a ton of money."

Moreover, as Ryne and Teargarden point out, firm-specific knowledge and ability is identified as "tacit knowledge." Polanyi (1967) and Kogut (1988) suggest this tacit knowledge provides competitive advantage since it is cumulative and slow to diffuse, as it is rooted in the firm's human assets (Rhyne and Teargarden, 1997) That is, it is a function of their culture, training, experience, and administrative heritage (corporate history). "This tacit knowledge is a key contribution of the skilled human assets variable to the value-added creation process."

The important point is that downsizing disrupts these informal networks and undermines the informal collaboration necessary for innovation. It "destroys informal bridges between departments, disrupts the information grapevine...and eliminates the friendships that bond people to the workplace" (Baker, 1996). It forces companies to reinvent the wheel, or spend time and money solving problems already solved in the past (van de Vliet, 1995). It also eliminates the firm's tacit knowledge, a key to competitive advantage. Consequently, it can debilitate high-technology organizations that depend on R&D and innovation for their survival.

Counting the True Cost of Employee Turnover

Although it negatively affects remaining workers, erodes loyalty, and weakens corporate memory, all these are only parts of the major problem with downsizing: It costs a ton of money. Researchers and businesses from all facets of the economy are reaching this same conclusion. High turnover rates carry all kinds of direct, indirect, visible, and hidden costs.

First are the visible, direct costs of turnover. These include advertising and marketing new positions; recruiting, hiring, relocating, and training new personnel, processing the paper work; paying overtime to employees taking up the interim slack; enduring the decrease in production as new employees learn their positions, paying unemployment claims, writing off the money spent training the

departed worker, and participating in meetings about departed employees (Positive Directions; Herman, 1997; "Turnover Costs," 1998; White, 1995; Manpower Bulletin, 1998; Birnbach, 1998; Fitzenz, 1997).

Second are the indirect, hidden costs of turnover. High rates of turnover cause multiple disruptions. Product delays occur in R&D, and potential manufacturing efficiencies are delayed or simply not reached. Customers are often lost, and quality, service, and morale decline. The company gets a reputation for its high turnover rate. Managers experience more stress, and work loads are increased in efforts to rebuild teams and the overall corporate culture. Moreover, these indirect expenses, which can amount to more than 80 percent of turnover costs, are rarely measured (Positive Directions; Herman; White).

Put these figures together and the cure is worse than the ailment. Estimates vary, but all demonstrate these high costs. Eric Rabinowitz, president of IHS HelpDesk Service, found that it cost $3,000 per person to bring on new hires. Kwasha Lipton estimates that replacing an employee costs an average of 150 percent of his salary for exempt workers, 175 percent for nonexempt workers. The Department of Labor estimates that replacing an employee costs one third of a new hire's annual salary. Others say a resignation costs about 1.3 times the annual salary of the one who left, others estimate anywhere from 25 to 200 percent of that salary, and still others say two to seven times annualized income.

Again, the Saratoga Institute has shown that on average, turnover costs for exempt employees are "a minimum of one year's pay and benefits, or a maximum of two years' pay and benefits." In a recent survey by William M. Mercer Inc., 45 percent of 206 medium-to-large U.S. companies reported that turnover costs more than $10,000 per employee replaced. Even a hamburger flipper at a fast food operation costs $500 dollars to replace, his manager $1,500. Regardless of the exact numbers or businesses, there is widespread agreement that turnover costs are somewhere between high and Olympian (Caggiano, 1998; Hansen, 1998; "Strategies for Managing Retention," 1998; Brannick, 1998; Birnbach; Herman; Fitzenz; Sunoo, 1998).

"Regardless of the exact numbers or businesses, there is widespread agreement that turnover costs are somewhere between high and Olympian."

The Emergence of the Strategy of Retention

As a result of the failures of downsizing, many companies and researchers have realized the value of retaining personnel and of achieving workforce stability. These analysts consider retention and stability not just a counterbalance to the excesses of downsizing, but a competitive strategy aligned with the realities of the volunteer workforce. Indeed, a review of the literature indicates that the effectiveness of this strategy is no longer an argument, but a given, and the question is no longer whether to implement it, but how to do it best.

Many companies now consider keeping good employees their number-one

problem. This is, as mentioned, at least partly a result of downsizing, which has made turnover so prevalent and problematic. Hundreds of companies and researchers have therefore examined why employees leave and how to keep them. Recruitment and retention replace downsizing and rightsiz-ing, with predictions that this pattern will remain for the foreseeable future. Experts now consider employee retention an essential competitive strategy (Caggiano, 1998; Positive Directions; "Strategies for Managing Retention," 1998; Moore et al., 1998; Herman, 1997).

"Many companies now consider keeping good employees their number-one problem."

This means most directly that retention affects the bottom line. The logic of this argument is actually rather straightforward and intuitively obvious. Businesses serve customers, and dissatisfied customers go elsewhere. Consistency and predictability of service build effective, efficient, productive business relationships. Experienced employees know the customers and their employees, and in general, the longer they are around the more familiar and steadfast those relationships become. This kind of strength is difficult to measure, but it seems obvious that longevity leads to knowledge that in turn leads to profit (Herman, 1997).

As a result, a number of people now examine the causes of turnover. The role of downsizing in turnover has been discussed. Employees cite a number of reasons, in addition to pay, for leaving a company. Indeed, in more than 50 surveys the Institute of Employment Studies has conducted over the past decade, only 10 percent cited pay as their main reason for leaving. Most often, they blame unchallenging work, poor management, little chance for promotion, rigid pay and benefits plans, and pressure (Bevan, 1997).

It follows, then, that there are correlating reasons why people stay. Craig Fuller, chairman of the National Chamber Foundation, states "there are three core values that affect whether people stay in their existing jobs...security, fulfillment, and membership." Security means not only a decent salary, but also involves child rearing, career management, and retirement plans. Fulfillment means not just a nice working environment, but flexible schedules, dress codes, and attitudes, and working for a respected company. Membership means employees believe they can contribute to the company's goals ("How to Keep Good Employees," 1998).

In short, people stay in places they are glad to work. Matt Weinstein, a consultant based in Berkeley, points out the realities of this new workforce, arguing that employers must consider their effective employees volunteers. Similarly, Ed McCracken, CEO of Silicon Graphics, suggests viewing these employees as consultants who primarily want challenging work (Lyons, 1997). It seems to come down to this: Employees want to perform engaging work for a respected company whose success they not only affect but also help define, and they want to do so in an environment that allows flexibility for other priorities. And today, managing a mobile, opportunity-laden, in-demand workforce with those desires is a necessity for competitive advantage.

The recognition of these realities—turnover rates are at about 1.1 percent a

month, the highest in 10 years—has led to a flurry of research and efforts designed to retain competent personnel. Booz, Allen and Hamilton, Inc., is just one of hundreds of companies implementing flexible pay systems and a variety of career development programs. Other companies have realized they not only need someone in charge of training, but also need someone in charge of retention. Yet others employ other strategies, including stock option plans, negotiable retirement plans, and sharing profits from production improvements (Bernstein, 1998; Champy, 1997).

In fact, retention is developing into a field of study as researchers and managers review the literature, implement strategies, and then revise understandings.

In a review of much of this literature, DeLeon (1997) shows how the connection between turnover and commitment has led 60 to 80 percent of Fortune 500 companies to try retention programs. Individually negotiated contracts (INCs), negotiable benefits packages, and tailored business systems (TBS) are some popular efforts. A number of managers and CEOs offer anywhere from 3- to 15-step methods of satisfying and retaining employees. The point here is not to delve into the mechanics of retention, but to demonstrate that its acceptance as a necessary and powerful competitive strategy is widespread (DeLeon, 1998; Herman; Sailors and Sylvestre, 1994; Scheier, 1997).

This thinking stands in stark contrast to the downsizing and outsourcing efforts so widely advocated today in much of the DoD. As Diana DeLeon states, recent developments in the commercial sector demonstrate that current public sector strategies "are not just old, they are inflexible, and many times without the employee in mind" (DeLeon, 1998). In the DoD, what some offer as innovative, cost-cutting certainties about the irreducible core are now seen to represent outdated failures in the private sector.

Moreover, it is ironic that the effectiveness of retention, recently utilized in the commercial sector, but yet to be discovered in the civilian side of DoD, has long been practiced by the military where commanders are responsible for bringing people on board properly, and for their training, development, and retention. Indeed, retention is now seen as one of the military's major problems. The DoD, it seems, can learn not only from the private sector, but also from what is going on outside its own front door (Champy, 1997).

"Indeed, retention is now seen as one of the military's major problems."

While downsizing may provide short-term advantages for a company and its shareholders, experts agree that the long-term drawbacks are significant enough to warrant exploring all other options first. As Bill Gandossy of Hewitt and Associates states ("Losing Corporate Memory," 1996), "The cloud hovering over the workforce, and the paralysis, suggests that it is not a good way to build a viable organization that will stay focused on growth and prosperity."

Implications for Lab Downsizing Efforts

Just as in the private sector, most of the downsizing in the DoD's in-house labs in

recent years has been driven by the belief that decreased headcount translates into money saved. If the only measure of that is the money spent on payroll, this might appear to be the case. However, as much of the private sector has now realized, there are other factors in the overall equation. Most of these, such as loss of corporate memory and high cost of turnover, have been discussed already.

Private sector experience has shown that, when all such costs are rolled up, downsizing does not usually create the savings its advocates claim. Rather, it often ends up costing more, which is precisely why it is becoming increasingly passé in the private sector. To illustrate: An American Management Association survey has found that fewer than 45 percent of the companies downsizing over the past 10 years have reported profit increases.

"As experiments, failure is not only allowed, it is a key aspect of success in allowing the system to be refined in the same environment it will ultimately be used."

Among the Association's member companies, downsizing and job elimination are at their lowest levels of the 1990s. In June of 1997, only 19 percent of those firms were engaged in downsizing, compared to 28 percent in June of 1996. Even the defense industry itself is beginning to cut costs by reforming processes rather than laying off employees. Stephen S. Roach, Chief Economist at Morgan Stanley and one of the staunchest promoters of corporate downsizing, now admits that "Corporate America can't rely on the 'hollowing' tactics of downsizing to maintain market share in an expanding global economy…I'm now having second thoughts as to whether we have reached the promised land" (Hansen, 1998; "Companies Target Processes," 1998; Roach cited in Nova, 1998).

It has already been seen that, in efforts to eliminate redundancies and cut costs, most private sector companies went about downsizing using what professor Kim Cameron calls a "grenade" strategy. This is very much the approach DoD labs have been forced to take in their downsizing efforts. Why? Because force reductions in a public sector enterprise are governed by civil service and other rules that make it nearly impossible to target reductions within the workforce. Where the downsizing triggers a reduction in force (RIF), a large number of employees may suffer collateral damage through the process known as bumping and retreating. In the end, who goes and who stays is often determined by seniority, veteran's status, or some other such factor.

And, while many reductions to date have been effected without RIFs, they have been implemented through a variety of "voluntary early retirement" and "separation incentive pay" inducements. These approaches too make it difficult for management to target the reductions within the workforce because it is difficult to know who will ultimately take such "buy-out" offers. In short, downsizing the labs under current rules is just as apt to result in the loss of a valued employee as the elimination of a truly redundant one.

Ironically, the loss of key technical personnel during the reduction process in the DoD labs has led to the necessity of recruiting new scientific and engineering

talent even as these labs collectively continue to shed end strength. That is, the DoD labs are currently experiencing just the sort of "churning environment" that Alan Downs said described Apple Inc. between 1985 and 1995, when "...the company lost its competitive edge, failing to develop a new breakthrough product during this entire period." This raises a disturbing possibility—will this churning environment in the DoD labs have a similar impact on their innovation and productivity?

This environment is likely to persist in the DoD labs for many years as already programmed "savings" from various outsourcing and end-strength reduction initiatives are pursued. Is it realistic to expect that these labs can recruit and retain the "best and brightest" scientific and engineering talent in this churning environment?

Again, private sector experience suggests they cannot. Even putting aside the current disparity in salary and benefit packages between the public and private sector, it seems increasingly unlikely these labs will be able to attract and retain the technical talent to support even a set of core functions. Scientists and engineers, like other employees, want more than a decent salary and flexible benefits. They also want a stable and fulfilling work environment where they can achieve both their personal and professional ambitions—a place where they are glad to work. After all, as much of the private sector has recognized, today's high-achievers are part of the "volunteer" workforce.

Indeed, evidence is accumulating that this environment is already taking a toll on the scientific and engineering (S&E) workforce at these laboratories. Data collected by the Defense Manpower Data Center shows that over the 7-year period ending in September 1997, the DoD laboratory S&E workforce experienced a 3-year gain in average age to 42.6 years. At the same time, the number of S&Es eligible to retire grew by 4 percent to more than a quarter of the workforce.

A sampling of data suggests that most turnover is taking place among the younger to mid-career S&Es. Many are simply resigning their government jobs and moving into the private sector. With much of the corporate knowledge in these laboratories resident in the S&E workforce that is retirement eligible, and with few younger S&Es replacing them, the future of these laboratories seems in considerable doubt.

"Scientists and engineers, like other employees, want more than a decent salary and flexible benefits."

Even so, the accumulating mountain of evidence from private sector downsizing experience seems to have had little impact on those who maintain that the work of these laboratories can and should be further restricted to some irreducible set of core functions. This notion rests on the private sector analogy where many companies have focused on a set of core competencies. But this seems a misinterpretation of the ideas set forth by the originators of the idea of corporate core competencies, say Gary Hamel and C. K. Prahalad (Hamel and Prahalad, 1990). They point out that a core competency is a distinguishing integration of the organization's resources (e.g., facilities,

people, processes, technologies, etc.) and collective knowledge in a way that contributes significantly to the perceived customer benefits of the company's products and services.

There is no mention in the Hamel and Prahalad (1990) definition of a core competence of the number of resources necessary for its creation and maintenance. That is, the number of resources underpinning a core competence may be as many or as few as needed. Moreover, a com-pany's core competencies embrace all of its in-house employees—a blue-collar employee on the shop floor can be just as important as a senior scientist in the R&D laboratory. Both are carriers of corporate core competence. This stands in contrast to the idea of the irreducible core as currently employed in the DoD labs, where many of the employees are not considered part of the core—their jobs, it is said, can be outsourced without damage to the remaining organization.

But the definition of core competence as put forth by Hamel and Prahalad, and practiced by numerous successful companies, shows that personnel reductions are just as likely to damage competencies as facilitate them. For one, reductions destroy corporate memory, a principal element of the know-how or collective learning of the organization and is an essential element of core competence. Interestingly, this assertion is buttressed by a recent meta-analytic review of 20 organizational studies of the relationship between organizational size and innovation. This review demonstrated a positive relationship between size and innovation (Damanpour, 1992). Less is not always more in an R&D-based organization.

In short, the current DoD laboratory environment is not conducive to the maintenance of core competencies, recruiting and keeping able employees, and fostering innovation. Neither is it likely to be conducive to saving money considering the impact on morale and productivity of the current tumultuous environment. Although the figures vary from place to place and the evidence at this point is largely impressionistic, it appears that only about 25 percent of scientists and engineers relocated after the latest round of base closures and realignments. Furthermore, many of those who did relocate subsequently left the government, an experience not unlike that observed in the private sector, where more than 35 percent of employees who were relocated left the company within three years (Oltman and Malinak, 1998). Who would spend $50,000—not to mention the additional costs of rehiring, retraining, and so on—on a piece of equipment that would be thrown out in three years? How could the DoD reconstitute capabilities after the loss of so much corporate memory and talent?

The DoD's search for the irreducible core could, like the hero in Greek tragedy, destroy what it seeks to preserve. In this case, the protagonist's greatest strength—its ability to produce the most efficient, effective, advanced military in the world—is the very source of its demise, as the near exclusive emphasis on economy drives costs up and talent away.

Michael L. Marshall has served as executive secretary of the Navy Laboratory/ Center Coordinating Group since 1992. Before that, he served the Director of Navy Laboratories (DNL) as special assistant for science and technology, and as head of the DNL's corporate projects office. He holds B.S. and M.S. degrees in physics and a J.D. degree in law.

(E-mail address: marshallml@nswc.navy.mil)

Eric Hazell has a Ph.D. degree in history from the University of Maryland, where he is an adjunct professor in the history and English departments. Since 1995 he has been the historian for the Navy's Research, Development, Test, and Evaluation Management Archives program. Other publications include "Panacea or Pipe Dream: Contracting Out Naval Research and Development since World War II," also co-authored with Mike Marshall (*Naval Institute Proceedings,* in press).

(E-mail address: Hazell.Eric@nhc.navy.mil)

REFERENCES

Allen, J. (1975, November). *Some changes in Department of Defense technology management.* (statement on the Department of Defense Laboratories).

Baker, W. E. (1996, May). Bloodletting and downsizing. *Executive Excellence.*

Bernstein, A. (1998, June 22). We want you to stay. Really. *Business Week.*

Bevan, S. (1997, November 20). Quit stalling. *People Management.*

Birnbach, R. (1998, July 27). Taming turnover: Retaining employees is best staffing strategy. *Puget Sound Business Journal.*

Brannick, J. (1998, April 28). *Decreasing the staggering costs of turnover in your organization.* http://www.florida-speakers.com/turnover-costs.htm

Brooking, A. (1999). *Intellectual capital.* International Thomson Business Press, Andover, England.

Bureau of the Budget. (1962, April 30). *Report to the President on government contracting for research and development* (Bell Report).

Bureau of National Affairs (1998, March 27). *Turnover climbed to 8-year high in 1997.* Press release. Washington, DC.

Caggiano, C. (1998, January). How're you gonna keep 'em down on the firm? *Inc.*

Cameron, K. (1997, Spring). Downsizing or dumsizing. *Brigham Young Magazine,* Vol. 51, No. 1.

Carlisle, R. (1996). Management of the U.S. Navy Research and Development Centers during The Cold War: A survey guide to reports. Navy Laboratory/Center Coordinating Group and the Naval Historical Center, Washington, DC.

Carlisle, R. (1997). Navy RDT&E planning in an age of transition: A survey guide to contemporary literature. Navy Laboratory/Center Coordinating Group and the Naval Historical Center, Washington, DC.

Carlisle, R. (1997). The relationship of science and technology: A bibliographic guide. Navy Laboratory/Center Coordinating Group and the Naval Historical Center, Washington, DC.

Champy, J. (1997, September 29). It's not who you hire, it's who you keep. *Computerworld.*

Chaurdron, D. (1994, December). After the layoffs: Healing and rebuilding. *HR Focus.*

Church, A. H., Cameron, K. S., Cascio, W. F., & Noer, D. M. (1995). From both sides now: Organizational downsizing: What is the role of the practitioner? *The Industrial-Organizational Psychologist, 33.*

Companies target processes, not workers, to cut costs. (1998, July 20-26). *Defense News.*

Coolidge, S. (1998, February 9). Managers who cut jobs may miss mark. *The Christian Science Monitor.*

Corporate amnesia. (1996, July/August). *The Futurist.*

Damanpour, F. (1992). Organizational size and innovation. *Organization Studies, 13.*

DeLeon, D. (1998, April 15). *Turnover.* http://jan.ucc.nau.edu/~gbh/soc631/paper3/3.14html

Department of Commerce. (1997). *America's new deficit: The shortage of information technology workers.* Washington, DC: Author.

Department of Defense. (1995, February). DoD Final Response to NSTC/PRD-1, Presidential Review Directive on an Interagency Review of Federal Laboratories. Washington, DC: Author.

Downs, A. (1996). *Corporate executions: The ugly truth about layoffs—How corporate greed is shattering lives, companies, and communities.* New York. AMACOM.

Dupuis, L., Boucher, S., & Clavel, L. (1996, August). Downsizing: Its effects on survivors. *Monograph.*

Fitz-enz, J. (1997, August). It's costly to lose good employees. *Workforce.*

Gemignani, J. (1998, April). Employee turnover costs big bucks. *Business and Health.*

Government Accounting Office. (1981, February 27). *The state of basic research in the DoD laboratories.* Washington, DC: Author.

Haggis, K. (1998, July 22). *Downsizing.* http://www.ucc.ucon.edu/~wwwiopsy/downsize.htm

Hamel, G., & Prahalad, C. K. (1990, May/June). The core competence of the corporation. *Harvard Business Review.*

Hansen, F. (1997, September/October). What is the cost of employee turnover? *Compensation and Benefits Review.*

Hansen, F. (1998, March/April). Downsizing and job cuts decline as major U.S. firms opt for growth. *Compensation and Benefits Review.*

Herman, R. (1997, June). Reducing costly employee turnover. *HR Focus.*

How to keep good employees from jumping ship. (1998, July 30). http://www.verexp.com/may20/voice.html

Jenkins, C. P. (1997, Spring) Downsizing or dumbsizing? *Brigham Young Magazine, 51*(1).

Kelly, J. (1998, July 29). *The loyalty contract: Employee commitment and competitive advantage.* http://ups.com/com/news/speech/loyalty.html

Kreiner, K., & Schultz, M. (1993). Informal collaboration in R&D: The formation of networks. *Organizational Studies.*

Langenbeck, E. (1982, August 1). Report to ASN(RE&S) on Navy RDT&E Centers. Department of the Navy. Washington, DC.

La Voie, A. (1997, November 6). *Downsizing may have ill effects on those still employed.* The Lancet Limited, London.

Lardner, R. (1998, August). The secret's out. *Government Executive.*

Losing corporate memory, bit by bit. (1996, May). *HR Magazine.*

Luker, W., & Lyons, D. (1997, June) Employment shift in high-technology industries, 1988–96. *Monthly Labor Review.*

Lyons, N. (1997, December). Managing the volunteer workforce. *Inc.*

McNamara, R. (1960, October 14). *In-house laboratories.* Memorandum.

Mone, M. (1994, Summer). Relationships between self-concepts, aspirations, emotional responses, and intent to leave a downsizing organization. *Human Resource Management.*

Mone, M. (1997, Fall). How we got along after the downsizing: Post-downsizing trust as a double-edged sword. *Public Administration Quarterly.*

Moore, J., Munzel, M., & Pfister, S. (1998, January/February). Are the keys to improving retention walking out your door? *The Human Resources Professional.*

Naval Material Command. (1983, July). *Research and development centers mission review panel support.* (Messere Report). Washington, DC: Author.

Noer, D. (1993). *Healing the wounds: Overcoming the trauma of layoffs and revitalizing downsized organizations.* Jossey-Bass Publishers, San Francisco.

Nova, S. (1998, July 24). *Countering corporate downsizing.* http://www.igc.apc.org/preamble/preface.html

Office of the Director of Defense Research and Engineering. (1966, October 31). *Department of defense in-house laboratories.* (Sheingold Report). Washington, DC: Author.

Oltman, D., & Malinak, D. (1998, July 29). *A study in employee turnover rates—Now you see them, then you don't.* http://www.erc.org/mobility/oltman.htm

Pinkovitz, W., Moskal, J., & Green, G. (1996-97, Winter). How much does your employee turnover cost? *Small Business Forum.*

Positive Directions, Inc. (1998, July 29). *Retain employees.* http://positivedirections.com/page6.html

President's Science Advisory Committee. (1958). Strengthening American science. Washington, DC: Author.

President's Scientific Research Board. (1947). *Science and public policy.* (Steelman Report). Washington, DC: Author.

Rhyne, L., & Teagarden, M. (1997, Fall). Technology-based competitive strategy: An empirical test of an integrative model. *Journal of High Technology Management Research.*

Sailors, F., & Sylvestre, J. (1994, March/April). Reduce the cost of employee turnover. *Journal of Compensation and Benefits.*

Scheier, R. (1997, September 8). Fifteen ways to keep your people. *Computerworld.*

Sharma, A. (1996, December). What's wrong with "rightsizing." *Manufacturing Engineering.*

Turnover costs. (1998, July 29). *SOHO Guidebook.* http://www.toolkit.cch.com/Text/PO5_7145.stm

Strategies for managing retention. (1998, July 29). *Manpower Bulletin.* http://www.psb.gov.sg/whatsnew/bulletin/bulletin_p2.html

Stum, D. L. (1998). *America @ Work: An overview of employee commitment in America.* AON Consulting Loyalty Institute, An Arbor, MI.

Sunoo, B. P. (July 1998). Employee turnover is expensive. *Workforce.*

Texas Department of Mental Health and Mental Retardation. (1998, April 28). *Turning employee turnover around.* http://www.mhmr.state.tx.us/hrs/news/hrll-1.htm

van de Vliet, A. (1995, January). Lest we forget. *Management Today.*

White, G. (1995, January). Employee turnover: The hidden drain on profits. *HR Focus.*

FROM CRADLE TO SAVE: *REVOLUTIONARY ACQUISITION FORCE STRUCTURE ALTERNATIVES FOR THE 21ST CENTURY*

Lt Col Craig Olson, USAF

Military strategists depict a future characterized by the uncertainty of when and where conflicts will emerge—requiring that U.S. forces be prepared to engage worldwide, with leading-edge technologies. This challenge cannot be met without a revolutionary change in the present acquisition force structure. The services have the tools in hand to meet this challenge; will the Department of Defense be able to make the needed changes?

> ***"There is nothing more difficult to carry out, nor more doubtful of success, nor more dangerous to handle, than to initiate a new order of things."***
>
> **—Niccolo Machiavelli**

The date is October 22, 2015, just one day after the new commander-in-chief (CINC), U.S. Pacific Command (CINCPAC) assumed leadership. Intelligence sources indicate that China has been aggressively developing a family of all-weather precision guided munitions (PGMs), which they have just begun producing in significant numbers. This observation, combined with growing indications of China's desire for regional hegemony, has brought Taiwan to the forefront of the PACOM's (Pacific Command) security challenges.

Upon careful analysis of the situation, CINCPAC decides to seize this opportunity to engage the PACOM Operational Experimentation Force (PACOM OPEXFOR), a key component of an "acquisition renaissance" which has evolved over the past 15 years. Knowing that automatic target recognition (ATR) technology has progressed dramatically in recent years, CINCPAC immediately tasks the OPEXFOR commander, whose tightly coupled joint team of requirements, acquisition, and operational specialists will define a requirement and engage with

industry to identify suitable emerging technologies and integrate the appropriate hardware and software upgrades into existing sea, land, and airborne sensor platforms.

CINCPAC is aptly impressed as he observes the self-contained, multidisciplined OPEXFOR team orchestrate a series of full-blown acquisitions in just 18 months. The CINC will complete his tour, confident his successor has at his or her command the first truly robust, theater-wide, joint combat identification network, capable of detecting, locating, identifying, and destroying Chinese assets well before they enter Taiwanese airspace, effectively rendering China's PGM inventory obsolete.

Though a scenario like this is not feasible for a major new system such as the F–22, it is indeed a reasonable goal for the development, integration, and initial fielding of the various system and subsystem hardware and software acquisitions that compose the majority of combat capability improvements.[1] Moreover, to turn such a scenario into reality, it is absolutely essential that we reevaluate our present acquisition and operational force structures. We, in fact, must create an integrated acquisition and operational force structure if we hope to organize, train, and equip our future forces with the same technological edge they have become accustomed to, thus allowing them to maintain a decisive advantage over any adversary in a future characterized by uncertain threats and rapid technology change (Gansler, 1998, p. 1).[2]

This article lays out a path ahead toward an "acquisition renaissance." First, however, I'll discuss the present state of acquisition reform and the status of operational experimentation programs. Next, three alternative acquisition force structures will be presented that exhibit varying degrees of coupling between the acquisition and operational communities (Figure 1). The advantage and disadvantage of each alternative will be examined and a recommendation made as to the optimum acquisition force structure to pursue. The discussion will occur exclusively at the strategic level with the purpose being to challenge the reader to seriously think through the opportunity for revolutionary change in our defense acquisition system. The fine details of the

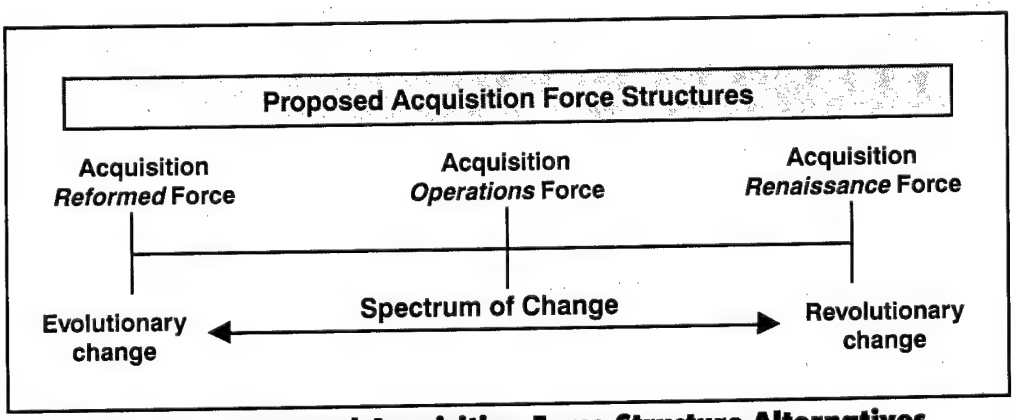


Figure 1. Proposed Acquisition Force Structure Alternatives

ensuing interagency, interservice, and cross-community changes and implications would be an interesting subject of a much more detailed study.

Reform or Streamlining? A Background of Improvement

Modern acquisition reform began in the early 1970s following growing public perception of Pentagon mismanagement during the Vietnam War (National Security Decision Making Department, 1998, pp. 4–5).[3] While acquisition reform initiatives in the 1970s and 1980s took place in the context of a rather predictable threat environment, more recent initiatives, such as the Defense Reform Initiative (DRI) of 1997, have attempted to align the defense infrastructure with a much more dynamic environment (Defense Reform Initiative, 1997, p. 1).[4] Collectively, these types of initiatives have emphasized an appropriate balance between oversight and efficiency and have been successful in reducing the cycle time of several noteworthy programs ("Executive Summary," 1998).[5] Another significant step in acquisition reform came from the institution of the advanced concept technology demonstration (ACTD) program, which has provided a means of bringing together the development community with the operational community to address emerging technologies as potential solutions to critical military needs (Gansler, 1998, p. 8).[6]

Improvement initiatives have unquestionably streamlined acquisition. But has there been true transformation, or is the reformed process of today just a modified relic of the Cold War era?[7] Our national security strategy and Joint Vision 2010 depict an uncertain future and demand U.S. military forces engage worldwide, throughout the conflict spectrum, with leading-edge technologies. This provides a challenge which simply cannot be met short of a revolutionary change in the present acquisition force structure.

The need for a true acquisition revolution has been captured well by Jacques S. Gansler, Under Secretary of Defense for Acquisition and Technology: "We must modernize our current weapons systems; develop and deploy the major new systems and subsystems required for 21st century operations; and support those systems efficiently, effectively, and securely—and we must do all three of these at lower cost and with drastically reduced cycle times."(Gansler, 1998, p. 2) The traditional acquisition corps, which will be even smaller in the future, cannot do this alone.[8] It must draw upon the resources available in the operational community, where opportunities abound in a series of operational experimentation and demonstration programs now taking place.

"Modern acquisition reform began in the early 1970s following growing public perception of Pentagon mismanagement during the Vietnam War...."

Operational Experimentation Programs

Seeing is believing. More than 400 years ago, Machiavelli recognized this when he said, "For the reformer has enemies in all those who profit by the old

order, and only lukewarm defenders in all those who would profit by the new order ...who do not truly believe in anything new until they have had actual experience of it" (Machiavelli, 1532/1952). Service operational experimentation programs initiated within the last few years have just begun to provide such an opportunity. Specifically, the Navy's Fleet Battle Experiments,[9] the Air Force's Expeditionary Force Experiments,[10] the Army's Advanced Warfighting Experiments,[11] the Marine Corps Warfighting Laboratory,[12] and finally, the interservice Joint Warfighting Experiments,[13] are taking those vital first steps toward institutionalizing a process of maturing emerging technologies in operational environments ("The New Naval War College," 1998; Cohen, 1997, p. 42; Lowrey, 1997; Krulak, 1996, Gansler, 1998, p. 5).

Each of the experimentation programs has a common goal—providing the capability to rapidly develop emerging technologies and new warfighting concepts and align them with new doctrine, tactics, techniques, and organizations (Cebrowski and Garstka, 1998; Krepenivich, 1994).[14] As experiments, failure is not only allowed, it is a key aspect of success in allowing the system to be refined in the same environment in which it will ultimately be used. In simple terms, evolutionary acquisition is occurring (Secretary of the Air Force, 1998, p. 2).[15] The experiments are always built around emerging technologies and innovative warfighting concepts, and each is directly linked to Joint Vision 2010. Thus, they represent the first legitimate attempts to bring together industry, acquisition, and operational communities in a single coordinated effort to advance the art of war.

"The experiments are always built around emerging technologies and innovative warfighting concepts, and each is directly linked to Joint Vision 2010."

With these powerful acquisition reform and operational exercise tools in the hands of each of the services, there would appear to be an almost unlimited potential to make sure the warfighter receives the right systems at the right time—like never before in the history of warfare. Will the Department of Defense (DoD) embrace this potential and begin to establish the appropriate force structure changes as we enter the 21st century? The discussion will now turn to alternative acquisition force structures that could capitalize on these unprecedented opportunities.

Alternative Acquisition Force Structures

Not unlike the rest of our federal government, the defense acquisition system is organized to provide an elaborate and necessary means of checks and balances.[16] As such, it has been successful in producing the world's most effective and lethal weapon systems. Unfortunately, effectiveness is not synonymous with efficiency. Even with the reforms discussed earlier, most would agree that the present system is still too cumbersome to be compatible with the rate of technology change and the uncertain security environment of the future. What follows is a strategic-level discussion of three alternative acquisition force structures.

Each will be examined with respect to its organizational structure (see notional diagrams in the Appendix, Figure 3), as well as its associated strengths and weaknesses.

Alternative I: Acquisition Reformed Force

The first alternative is termed the acquisition reformed force. As the title suggests, it is characterized by an evolutionary extension of the present trends in the acquisition and operational communities. In the acquisition reformed force, each community will continue to aggressively pursue improvements in the areas outlined previously, but they will maintain a separate and distinct chain of command, just as they do today.

For the purposes of this discussion, the acquisition community includes headquarters (Pentagon), program office, research, and industry arms.[17] Program managers continue to report to program executive officers (PEOs), while supporting requirements inputs from the operational commands. The tour length for the typical program manager is longer to ensure continuity through the acquisition cycle. It is assumed that defense reform initiatives have been successfully implemented, allowing business affairs within DoD to be nearly as streamlined as those in the civilian sector, resulting in significantly reduced overall contract award and execution timelines when compared to today.[18]

Due to a significantly reduced government research and development capacity, the Acquisition Reformed Force will rely heavily on the civilian sector for innovative technologies. Successful streamlining has increased the ease of doing business with the government, resulting in a preponderance of healthy competition from technology-rich vendors of all sizes. Furthermore, due to the shrinkage of the acquisition workforce, contractors have been empowered with the bulk of the engineering and program management responsibility. They are "monitored" rather than "managed" by the program offices. An evolutionary acquisition approach is used in many cases, but it is not common across the services. Personnel within the acquisition community will function basically as they do today—geographically and service separated, with little awareness of the intricacies of each other's specialties and requirements.

"Successful streamlining has increased the ease of doing business with the government, resulting in a preponderance of healthy competition from technology-rich vendors of all sizes."

Like the acquisition community, the operational community in the acquisition reformed force has also matured in its ability to identify new technologies and evaluate their suitability. Service OPEXFORs have been institutionalized and are under the control of service operational commands. Planning and performing the experiments is the primary responsibility of operational test and evaluation (OT&E) specialists, although they are heavily supported by the development test and evaluation (DT&E) community. They occur approximately once each year and consider technology applications across the whole spectrum of conflict. Many, but not all, new technologies are evaluated in the service experiments (OPEXs). Occasionally a joint operational experiment will

take place, but for the most part, technologies are identified and evaluated based on individual service needs.

As an acquisition force structure for the future, the primary advantage of the acquisition reformed force is its relatively low risk.[19] Since many of the characteristics of this force structure are just beginning to be apparent today, there will be few remaining bureaucratic or parochial hurdles to overcome for it to succeed in offering at least some improvement in efficiency.

The low risk is also its primary disadvantage, as there is little likelihood for a dramatic improvement in DoD's ability to procure systems faster, better, and cheaper. Furthermore, although to a lesser degree than in the past, a distinct possibility still exists for the procurement of a system that does not adequately meet user needs, is unnecessarily service-unique, or is not interoperable. Finally, future personnel drawdowns will leave a smaller acquisition and operator workforce available to support this structure, leaving the acquisition reformed force with little choice but to work harder with less, not unlike the frustrated forces of today.

"As an acquisition force structure for the future, the primary advantage of the acquisition reformed force is its relatively low risk."

Alternative II: Acquisition Operations Force

An institutionalized, interagency focus characterizes the acquisition operations force. Essentially, this force structure takes many of the positive aspects of the acquisition reformed force, and formalizes them across the services. It includes all the acquisition and OPEX initiatives of the acquisition reformed force, thus these efficiencies are also present in the acquisition operations force. Finally, it brings together most of the acquisition and operational specialists into a single organization, under a single commander.

In the acquisition operations force, the program office is still the focal point of the procurement process, but it is organized very differently from today's program offices. A senior military or civilian program manager will direct the program, and he or she will typically be an acquisition specialist. Though not common, a program manager will occasionally come from an operational background. In a significant departure from the acquisition reformed force, the program manager will report to an appropriate operational commander instead of the PEO (e.g., Air Combat Command for the F–22 program).

In light of the huge drawdown in acquisition personnel highlighted earlier, the acquisition operations force has embraced the need for radical restructuring at the program office and Pentagon level. Program offices will include a mix of operational specialists to complement a reduced staff of the typical program personnel. The operational specialists will perform the requirements definition function presently performed within the operational commands, and they will assist the acquisition specialists as they interface with the Pentagon (e.g., program objective memorandum development).

The Pentagon staff will rely heavily on increased program office support since they have taken most of the acquisition

personnel cuts. The PEO and program element monitor (PEM) staffs will be merged, and the functions of these staffs will be shared with the restructured program office.[20] Finally, there is no longer a need for separate DT&E and OT&E test specialists since all test functions will fall under the program manager.

An evolutionary approach is the standard practice in the acquisition operations force—across the services and in all new acquisition programs. Furthermore, it is well-understood and accepted by the defense industry. Consequently, ACTDs are no longer necessary as a separate means of quickly demonstrating and fielding new technologies. The evolutionary approach is fully complemented by an increased emphasis on operational experimentation in comparison to the acquisition reformed force.[21] Service OPEXs occur at a minimum of twice each year, and they have a more joint focus. Furthermore, joint warfighting experiments are the rule rather than the exception, and they take place at least once every two years. Finally, successful evaluation of all new system and subsystem programs in at least one of the OPEXs is a mandatory exit criteria for advancement in the acquisition process.

The primary advantage of the acquisition operations force is unity of command. A single operational commander overseeing the procurement process offers the distinct advantage of placing the ultimate responsibility for the suitability of a system where it belongs—on a single person who represents the user. Obviously, he or she must be supported by a balance of acquisition and operational specialists. For example, the operational commander might have two vice/deputy commanders—one for operations and one for procurement. In any case, this approach should limit the finger-pointing that goes on today between the acquisition and operational communities. Moreover, "requirements creep" will no longer be a curse. It may even be embraced as an inherent aspect of an uncertain security environment and fully accommodated by the evolutionary acquisition approach and frequent OPEXs (Wall, 1998).[22] The evolutionary approach, combined with fully merged DT&E and OT&E functions, also offers the potential of dramatically reducing the overall development time for a system or subsystem.[23]

"The primary advantage of the acquisition operations force is unity of command."

The primary disadvantage of the acquisition operations force is the significant paradigm shift required for it to be implemented successfully. At present, there is a clear separation between the acquisition and operational communities. Operators typically have little appreciation for the complexities of acquisition and test, and this is exacerbated by the lack of operational experience among the majority of acquisition specialists.[24] Furthermore, there is often very little interest among operators in becoming involved in the acquisition community. Many would argue that this arrangement is as it should be, since it provides a necessary balance to the overall procurement process. This benefit does not have to be sacrificed, as a system of checks and balances will still occur within the acquisition operations force, but now in a compressed fashion.

A second disadvantage of the acquisition operations force is an inherently reduced opportunity for oversight, specifically the type presently provided by PEO/PEM staffs and operational command requirements staffs (Gansler, 1998, p. 8).[25] Consequently, although systems may be delivered faster, there is less of a guarantee they will also be consistently better or cheaper. Reduced oversight does not mean "no oversight," however, staff size and composition will have to be chosen very carefully. Other factors to consider in choosing the optimum Pentagon and operational command staffs include:

"Reduced oversight does not mean no oversight, however, simply that staff size and composition will have to be chosen very carefully."

- balancing the authority of operational commanders with senior Pentagon acquisition officials regarding requirements versus budget;
- determining how budget cuts are spread among programs; and
- deciding where responsibility should lie for answering congressional inquiries.

The solutions to these challenges merit further study, but they should not be considered insurmountable. Rather, they are the type of challenges one should expect with a large paradigm shift.

Finally, the acquisition operations force still maintains a distance between the acquisition process and the ultimate warfighter—the CINC and his forces. Consequently, there is still a finite possibility of a system being delivered that is not adequately "joint," interoperable, or optimized for the mission at hand.[26]

Alternative III: Acquisition Renaissance Force

The final acquisition force structure alternative to be developed is termed the acquisition renaissance force. As the name implies, it represents a dramatic departure from the present paradigm of procuring systems. Like the other two alternatives, it includes the efficiencies of defense reform and operational experimentation programs as a standard framework. This force structure is unique, however, in that it shifts the focus of acquisition efforts to the ultimate warfighters, the CINCs of the Unified Commands, thus providing both an operational and a joint focus to procurement.

The simplest way to envision the key characteristic of the acquisition renaissance force is as a self-contained program office, analogous in structure to that of the acquisition operations force, but assigned to the CINC as part of his or her designated staff (e.g., J-xx). It would be headed by a flag officer who is supported by senior program management and requirements officers from each of the services. In contrast to the other two alternatives, these program managers and requirements officers are no longer considered specialists, but rather "renaissance" professionals with savvy in both arenas. How is such a broad range of expertise obtained? It occurs through an increased cross-flow between the communities throughout an officer's career. It is

assumed that the great majority of officers in this force structure begin their careers as operators, and then branch off into acquisition-related jobs at the mid-career point. These officers are then expected to move between acquisition and operational positions as they progress in rank. The experience gained from cross-flow will be augmented by specific training (e.g., a short program management or test and evaluation course taught at the Defense Systems Management College).

The size of the program office branch will be dependent on the scope of operations and the equipment apportioned to the CINC, but in all cases it would be larger than the typical program offices today, since it would likely be responsible for a wide variety of programs. The acquisition renaissance force assumes that the evolutionary acquisition approach is fully embraced, and a great majority of hardware and software acquisitions will have a relatively quick cycle time (i.e., less than three years), commensurate with a CINC's strategic horizon.[27] The services will maintain Title X responsibilities and budgets to organize, train, and equip their forces. In addition, a reduced Pentagon staff, analogous to that in the acquisition operations force, will also remain in place. This staff will coordinate with the Pentagon Joint Staff to determine the disposition of all acquisitions.

In addition to the program office branch, the acquisition renaissance force will also include an OPEXFOR as part of the CINC's designated staff, (e.g., J-xx+1). This branch will include all the test personnel (who, again, will have mixed acquisition and operational backgrounds), and it will be responsible for planning, executing, and evaluating the results of each OPEX. In contrast with the other two alternatives, OPEXs will no longer be service-unique but rather shared between the CINCs, as designated by the Pentagon Joint Staff.

The primary advantage of the acquisition renaissance force is that it provides an inherently joint focus while placing the responsibility for procurement in the hands of the ultimate user, the warfighting CINC. The CINC is also the individual most concerned with the security environment, and is therefore highly motivated to ensure the right system is delivered at the right time. By the same token, operators will be intimately involved in the acquisition process from the outset, significantly reducing the potential for a system requirements mismatch. Another advantage of the acquisition renaissance force is the higher potential of successfully accommodating the drawdown in acquisition specialists. This alternative fully embraces a dramatically reduced workforce, and grooms and trains personnel to best adjust to it. Furthermore, it provides a means of more tightly coupling the joint strategic planning system (JSPS) activities with the planning, programming, and budgeting system (PPBS) activities, thus enabling a closer match between CINC priorities, program objective memorandum development, and systems acquisition.

"The primary advantage of the acquisition renaissance force is that it provides an inherently joint focus while placing the responsibility for procurement in the hands of the ultimate user, the warfighting CINC."

Clearly, the primary disadvantage of the acquisition renaissance force is risk. Indeed, it is the highest risk approach of the three alternatives presented. Although it offers a framework most likely to accommodate rapid concurrent development of new technologies and appropriate operational systems, it runs the risk of developing systems too quickly. Furthermore, since CINCs traditionally focus out from one to three years, this approach will tend to deemphasize long-range planning. The result could easily be suboptimum expenditure of funds on acquisitions that are short-term fixes applicable only to theater-specific scenarios. Allowing the services to maintain Title X responsibilities will provide a means of controlling this tendency; nevertheless, great care must be taken to ensure that checks and balances are put in place between the unified commands, operational commands, and the Pentagon staffs.

"Care must also be taken to ensure that personnel are adequately trained to maintain acquisition and operational expertise, and that enough of these new "renaissance specialists" are available for this option to succeed."

This approach also requires a huge paradigm shift, even larger than the case of the acquisition operations force. Extra caution must also be exercised as the traditional program offices are totally restructured and reassembled underneath the CINC. Staffs must be sufficiently streamlined given the available personnel, but not made so small that program managers are overburdened with too many diverse programs. Care must also be taken to ensure that personnel are adequately trained to maintain acquisition and operational expertise, and that enough of these new "renaissance specialists" are available for this option to succeed.[28] Finally, the tight coupling with industry achieved by the other two alternatives will be complicated by this approach simply due to geographic separation. Therefore, a widespread and robust secure and unsecured voice, video, and data network will be essential. It will also require a willingness on the part of industry personnel to travel in theater to support their equipment in OPEXs.

The Time for an Acquisition Revolution is Now

Having identified the characteristics of three alternative acquisition force structures, what remains is a basis upon which to judge them and recommend a preferred path toward the future. Many other permutations of the alternatives presented are certainly possible. Moreover, the strengths and weaknesses discussed should not be considered sacrosanct or all-encompassing. They are relative characteristics with respect to each alternative and only apply within the context of the grand strategy and security environment presented. The three alternatives presented were chosen simply because they span a spectrum running from an acquisition, or business-focused structure, to an operationally focused structure. As the advantages and disadvantages of each approach are laid out, they also tend to occupy ends of a spectrum (see Figure 2). Therefore, the

spectrum can be analyzed with the goal of choosing an acquisition force structure most appropriate for the context presented.

The acquisition reformed force occupies one end of the spectrum as the most business-focused. It is the lowest risk approach, but it also has the slowest cycle time, is the least "joint," and requires the largest number of personnel. Finally, it places the acquisition process furthest from the warfighter. The acquisition renaissance force, on the other hand, is the most operationally focused. It involves the highest risk, but also has the potential for the fastest cycle time. Furthermore, it offers the maximum degree of jointness and should require the fewest total personnel. The acquisition operations force falls on the spectrum between these two, although not necessarily in the middle.

In the context of the security environment presented—one of significant U.S. engagement in a world of high uncertainty, a broad range of threats, and rapidly emerging technologies—the key attributes of an optimum acquisition force structure are operational focus, rapid cycle time, and flexibility. Based on this argument, the acquisition renaissance force would appear to be the best acquisition force structure for the future. However, risk must also be considered, given the typically risk-averse nature of the U.S. military. The skepticism likely to be encountered with this high-risk approach might make it difficult to embrace, at least initially. Therefore, the most appropriate force structure to pursue at this time is likely somewhat different from the one presented here, perhaps a combination of the acquisition operations force and the acquisition renaissance force.

As already stated, significant further study is required to work out the details of any such restructuring. The reader is again reminded that the purpose of the argument has not been to focus attention on the merits of such details, but rather to encourage a serious consideration of the

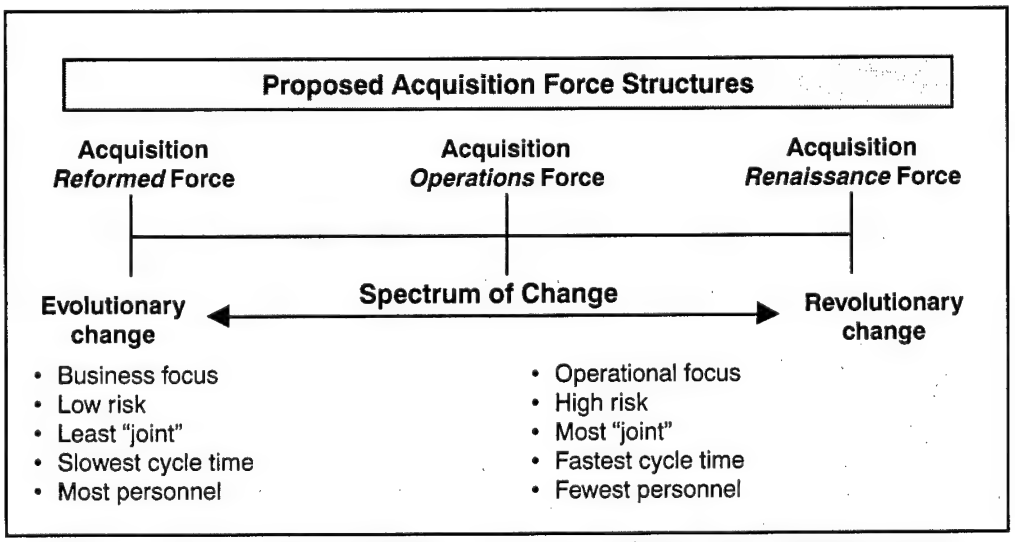


Figure 2. Spectrum of Alternative Acquisition Force Structures

opportunity for revolutionary change in our defense acquisition system. The time for holding on to old or slightly modified ways of doing business is past. An uncertain but dynamic future awaits the 21st century military leader. It calls for an equally dynamic approach to system procurement.

"The only thing harder than getting a new idea into the military mind is getting an old one out."
—B. H. Liddell Hart

Lt Col Craig S. Olson, U.S. Air Force, is presently assigned to the Secretary of the Air Force for Acquisition, Special Programs Directorate, in Washington, D.C. He is a graduate of DSMC's APMC 99-3. His background includes operational flying tours as an F–4 weapon systems officer and electronic warfare officer, as well as a flight test tour in the F–15E. He has also served as a program manager in the Joint STARS Joint Program Office. He holds an M.S. degree in mechanical engineering from Boston University and a B.S. degree in engineering mechanics from the U.S. Air Force Academy. In addition, he is a graduate of the U.S. Air Force Test Pilot School, the Air Command & Staff College, and the Naval War College.

(E-mail address: craig.olson@pentagon.af.mil)

REFERENCES

Cebrowski, A. K., & Garstka, J. J. (1998, January). Network-centric warfare—its origin and future. *U.S. Naval Institute Proceedings,* 35.

Cohen, W. S. (1997, May). Secretary of Defense, *Report of the Quadrennial Defense Review. Washington,* DC: Office of the Secretary of Defense.

Department of Defense. (1977). *Defense Reform Initiative, the business strategy for defense in the 21st century.* Washington: Author.

Executive summary of arsenal ship report. (1998, March 2). *Inside the Navy,* p. 10.

Gansler, J. S. (1998, March 12). Testimony before Senate Subcommittee on Acquisition and Technology, Committee on Armed Services, by Under Secretary of Defense for Acquisition and Technology. 105th Cong., 2d Sess.

Krepenivich, A. (1994, Fall). Cavalry to computer: The pattern of military revolutions. *The National Interest.*

Krulak, C. C. (1996, Autumn). Operational maneuver from the sea: Building a Marine Corps for the 21st century. *National Security Studies Quarterly,* 19–29.

Vern Lowrey, (1997, November). Army division advanced warfighting experiment. *Engineer,* 27.

Machiavelli, N. (1952). Book 6. Of new dominions which have been acquired by one's own arms and ability. In *The Prince* (pp. 49-50). New York: New American Library. (Original work published 1532)

National Security Decision Making Department. (1998, August). *Resource allocation, the formal process* (2nd ed.). Newport, RI: U.S. Naval War College.

Secretary of the Air Force. (1998, April 30). *Evolutionary acquisition process for C2 systems* (Air Force instruction 63-XXX [Draft]). Washington: Author.

The New Naval War College, Focusing on Forward Thinking. (1998, September/October). *Surface Warfare,* 4 (Navy Warfare Development Command Maritime Battle Center).

Wall, R. (1998, August). Expeditionary nerve center. *Air Force Magazine,* 66.

ENDNOTES

1. The argument will focus on organizational, or force structure, changes that could institutionalize a dramatic reduction in the program definition and engineering and manufacturing development phases of the acquisition cycle for typical system and subsystem upgrades. The length of these phases for a traditional acquisition of this type usually ranges from two to five years, depending on the size and complexity of the system or subsystem. This study focuses on an organizational structure that will reduce the cycle by at least 50 percent. The study does not directly address other potential areas of change, such as funding availability and stability (i.e., program objective memorandum development) which, though considered important, are beyond its scope.

2. Although we obviously cannot be sure of the security environment we will face in the next 10 to 20 years, it is likely to be dramatically different and far more dynamic than that provided by the Cold War. One only has to look at a short list of the activities in which the U.S. military has been engaged since 1990 to confirm that this is already the case: conventional war in Desert Storm, humanitarian relief and urban warfare in Somalia, peacekeeping in Bosnia, the riots in Los Angeles, and the recent attack against terrorist facilities in Afghanistan and Sudan—nearly the entire spectrum of conflict is covered. Moreover, we have had to face these challenges while undergoing a significant drawdown in force structure and a declining budget—two characteristics unlikely to change without the presence of a large peer competitor. Some of the specific characteristics and players of the early 21st century security environment will likely include: emerging democracies, potential competing major powers, rogue actors with weapons of mass destruction (WMD), large nonstate criminal organizations, and increasing economic and informational interdependence. Future adversaries probably will not attempt to directly combat the technologically superior U.S. military in a force-on-force sense, but will rather organize, train, and equip their forces to fight asymmetrically. Occurring simultaneously with these security environment changes is technology change at a rate never before witnessed in history. In sum, the future represents a set of constraints and opportunities that demand a fundamental change in our means of procuring systems.

3. The first DoD 5000-series documents were written in this time frame. These provided key guidance in several areas, including: increased oversight at distinct acquisition "phases," a requirement for Secretary of Defense approval at three decision milestones (program initiation, full-scale development, and production and deployment), the use of existing military or

commercial capabilities to satisfy mission needs whenever possible, and minimizing documentation. Many adjustments to the 5000-series documents have occurred since then, but the focus has continued to be increased efficiency and effectiveness through such principles as a streamlined or reduced number of management levels, centralized policy with decentralized execution, use of prototypes, and operational test and evaluation. In addition, the Packard Commission created, among other things, the defense acquisition boards (DAB) as a forum for increased oversight of programs at major decision milestones.

4. With respect to acquisition, DRI focuses on the need for DoD to adopt the "revolution in business affairs" which has allowed the American commercial sector to maintain a competitive edge in the rapidly changing global marketplace. Among these initiatives are more open government-contractor relationships as well as greater empowerment of the contractor, paperless contracting processes, electronic catalogs, discontinued printing of all DoD-wide regulations and instructions (to be made available exclusively through the Internet or CD-ROM), and reductions in military specifications.

5. Before cancellation, the Arsenal Ship program had demonstrated a 50 percent reduction in acquisition time for the design portion of the ship compared to traditional design approaches. This was primarily enabled by using industry-led acquisition operating under 110 *U.S. Code* Section 845 authority, which gives industry full trade space and responsibility for the design. In the Joint Direct Attack Munition (JDAM) program, streamlining initiatives saved $3 billion in program cost, decreased production delivery time by 48 months, and increased the warranty from 5 to 20 years.

6. ACTDs have provided an unprecedented opportunity to evaluate military utility prior to committing to formal acquisition (usually in a field demonstration or operational deployment), while developing appropriate concepts of operation and doctrine. Additionally, ACTDs often result in availability of an asset with a limited operational capability at the conclusion of the program while production models are developed. Since 1994, 46 ACTDs have been initiated, and the first nine were completed in an average time of about 20 months (concept to prototyping, assessment, and fielding of a limited capability). As would be expected, ACTDs have resulted in programs that transition to the formal acquisition process and programs that were terminated. Examples include the Kinetic Energy Boost Phase Intercept (BPI) program and the *Predator* unmanned aerial vehicle (UAV). The BPI ACTD, which evaluated the affordability, operational utility, and mission effectiveness of BPI engagements of tactical ballistic missiles, was terminated after determining that it was technically feasible but not operationally affordable. The

Predator, an unmanned aerial reconnaissance platform, was considered suitable and has actually entered the formal acquisition process while continuing to support peacekeeping operations in Bosnia.

7. The acquisition process in place during the Cold War produced highly effective technologies and systems (e.g., stealth, Joint STARS, PGMs), but it has not consistently demonstrated the ability to keep pace with rapid technology change.

8. Change is all the more critical in light of the upcoming reduction in personnel—124,000 fewer in the acquisition corps and 12,500 fewer in DoD Headquarters (as well as a 20 percent reduction in the government laboratory and test and evaluation infrastructure by 2005). The cuts in personnel and reductions in T&E infrastructure are to be implemented by the Defense Reform Act of 1997 and the Fiscal Year 1996 Defense Authorization Act, respectively.

9. The U.S. Navy is using a series of fleet battle experiments to turn their 21st century vision of network-centric warfare into reality. Specifically, they are using new information technologies to combine sensor, command and control, and engagement grids into a joint fires coordination network, or "ring of fire."

10. The U.S. Air Force has established an Expeditionary Force Experiment (EFX) program to complement the work ongoing at its six battle labs. They recently completed their first annual experiment (EFX '98), which incorporated new technologies and concepts into combined live-fly/simulated Air Expeditionary Force (AEF) with the objective of evolving its core competencies on a foundation of global battlespace awareness and advanced command and control.

11. The U.S. Army has established a digitized heavy force called the Experimental Force (EXFOR) to carry out their Advanced Warfighting Experiments (AWE), where many of the Army's Force XXI information dominance and dominant maneuver initiatives are already being tested.

12. The Marine Corps considers its Warfighting Laboratory one of its most important initiatives. Through a series of Sea Dragon tests, they hope to combine new technology with innovative new organizations, doctrine, and training to create a force capable of dealing with changing operating environments. Among those to be looked at include power projection in the littoral battlespace, urban warfare, and crisis response focused on containing or obviating an incipient major theater war. Furthermore, it is forming a Special-Purpose Marine Air-Ground Task Force (Experimental) to begin integrating the ideas generated in the Warfighting Laboratory with the overall Marine Corps combat development process.

13. Though not as robust as the service experimentation programs, a joint warfighting program has also been

established specifically to help achieve the full spectrum dominance goal of Joint Vision 2010. A nominal amount will be invested in joint warfighting experiments ($23.7 million in fiscal year 1999) to provide field-demonstrated concepts and prototypes and to develop tasks, procedures, techniques, training, and doctrine that joint forces will need to realize Joint Vision 2010.

14. The service experimentation programs are neither operational exercises nor laboratory demonstrations. Rather, they are experiments conducted by actual operators in operationally relevant scenarios, often leaving behind a limited operational capability for the field. Vice Admiral Arthur K. Cebrowski, President of the Naval War College, emphasizes the importance of operational experimentation in facilitating concurrent development of technology, organization, and doctrine. He states, "In spite of a ponderous acquisition process, technology insertion is ahead of and disconnected from joint and service doctrine and organizational development... A process for the coevolution of technology, organization, and doctrine is required."

    Andrew Krepenivich further argues that because we are in a unique period of technology change, we may be in the midst of a revolution in military affairs (RMA)—a time when technological change, systems development, operational innovation, and organizational adaptation combine to fundamentally alter the character and conduct of war. The details of an RMA and whether or not we are in one was purposefully not be debated here. Such revolutions throughout history have not been recognized until after they have occurred. What is emphasized here is the importance of timely adaptation of operational and organizational concepts with technology change to allow us to at least reap the rewards of an RMA, should it occur—"a dramatic increase—often an order of magnitude or greater—in the combat potential and military effectiveness of armed forces."

15. Though such an approach is not new (it has been common in the commercial sector since the 1970s), it has not gained widespread interest in DoD until recently. The Air Force is in the process of formalizing "evolutionary acquisition" as part of the buildup for the annual EFX. Also termed "spiral development," this process attempts to more tightly couple the acquisition and operational communities. It was initiated in 1996 at the Air Force Electronic Systems Center. It is an iterative strategy for command and control (C2) systems that facilitates rapid operational assessments of new technologies, refinement of user requirements, and fielding of sustainable prototypes with operational utility. It is distinguished from the ACTD process in that it accepts requirements and technology change as key components of systems evolution, and allows systems to mature via 18-month development increments, or "spirals," into fully fielded systems.

16. The defense acquisition system has traditionally comprised the planning, programming, and budgeting system (PPBS), which determines which systems will be procured and how many, and the acquisition management system (AMS), which determines how the systems will be developed and produced. The PPBS and AMS intersect at the requirements generation system (RGS), which determines what systems will be procured and why.

17. The typical program office consists of program management, engineering, contracts, and finance specialists, similar to today, and it is supported by development, test, and evaluation (DT&E) specialists, who may or may not be located at the same site.

18. This is a critical assumption to the argument. If defense reform does not lead to dramatic increases in efficiency analogous to the civilian "revolution in business affairs," the improvements presented here obviously will not be as significant. The merits of the Defense Reform Initiative and its probability of success are topics for another study.

19. For the purposes of the alternative force structures presented, risk is measured as a degree of departure from existing methods of acquisition and is only meaningful as a relative measure between the alternatives. The risk analysis is not meant to be robust, but rather just one of several elements of comparison between alternatives.

20. The Joint Requirements Oversight Council (JROC) and joint warfighting capabilities assessment (JWCA) structures will remain in place to harmonize requirements between programs and services.

21. The evolutionary approach will have to be thoroughly documented in a series of joint instructions and backed up by revisions to the *Federal Acquisition Regulations* (FARs).

22. It could also be argued the increased number of OPEXs in the acquisition operations force will be cost prohibitive. However, the potential payback must also be considered. At present it is too early to quantify, but the promise is encouraging. Regarding EFX, for example, Maj Gen John W. Hawley, commander of the newly formed Air Force Air and Space Command & Control Agency, has said: "If we learn something from this experiment that allows us to make just one better budget decision, we'll likely save the American taxpayers the cost of this experiment and much, much more."

23. Since evolutionary acquisition is based on actually fielding incremental capabilities, the production phase is effectively shifted to the left. Consequently, since time equates to money, there is also a significant potential for cost savings.

24. With the exception of test pilots and navigators, few people acquire true expertise in both arenas. Pilots and navigators from each service usually

remain in the acquisition corps after completing either the Air Force or Navy Test Pilot School. This is not as true for naval aviators, who usually return to the fleet. Test pilots and navigators, however, account for a very small portion of the total acquisition corps.

25. Time itself can often be a check and balance, as has been demonstrated by ACTDs that are not adequately scrutinized before being operationally deployed. The *Predator* UAV ACTD is an example of this. It was designed to demonstrate unmanned aerial reconnaissance and was actually deployed to support operations in Bosnia, but was arguably not operationally suitable. Although an ACTD version of the *Predator* was developed in minimum time, its sensor suite had very limited capability, and there were several maintenance and sustainment challenges. Operations in Bosnia demonstrated the need for several improvements, resulting in many changes to the production system and approximately double the cost over the ACTD version.

26. The "jointness" and interoperability of the types of system and sub-system improvements which are the focus of this study will be heavily reliant upon the successful implementation of ongoing defense information infrastructure/common operating environment (DII/COE) initiatives, which should provide common hardware and software architectures upon which to place incremental upgrades.

27. Obviously, the CINC program office branches will not oversee all acquisitions. There will still be a need for CONUS-based program offices to handle major systems and subsystem acquisitions (e.g., Joint Strike Fighter).

28. To some extent, the Navy already takes this approach to acquisition (Navy test aircrews routinely cycle between operational and acquisition assignments), so it should be possible for other services to do the same.

APPENDIX

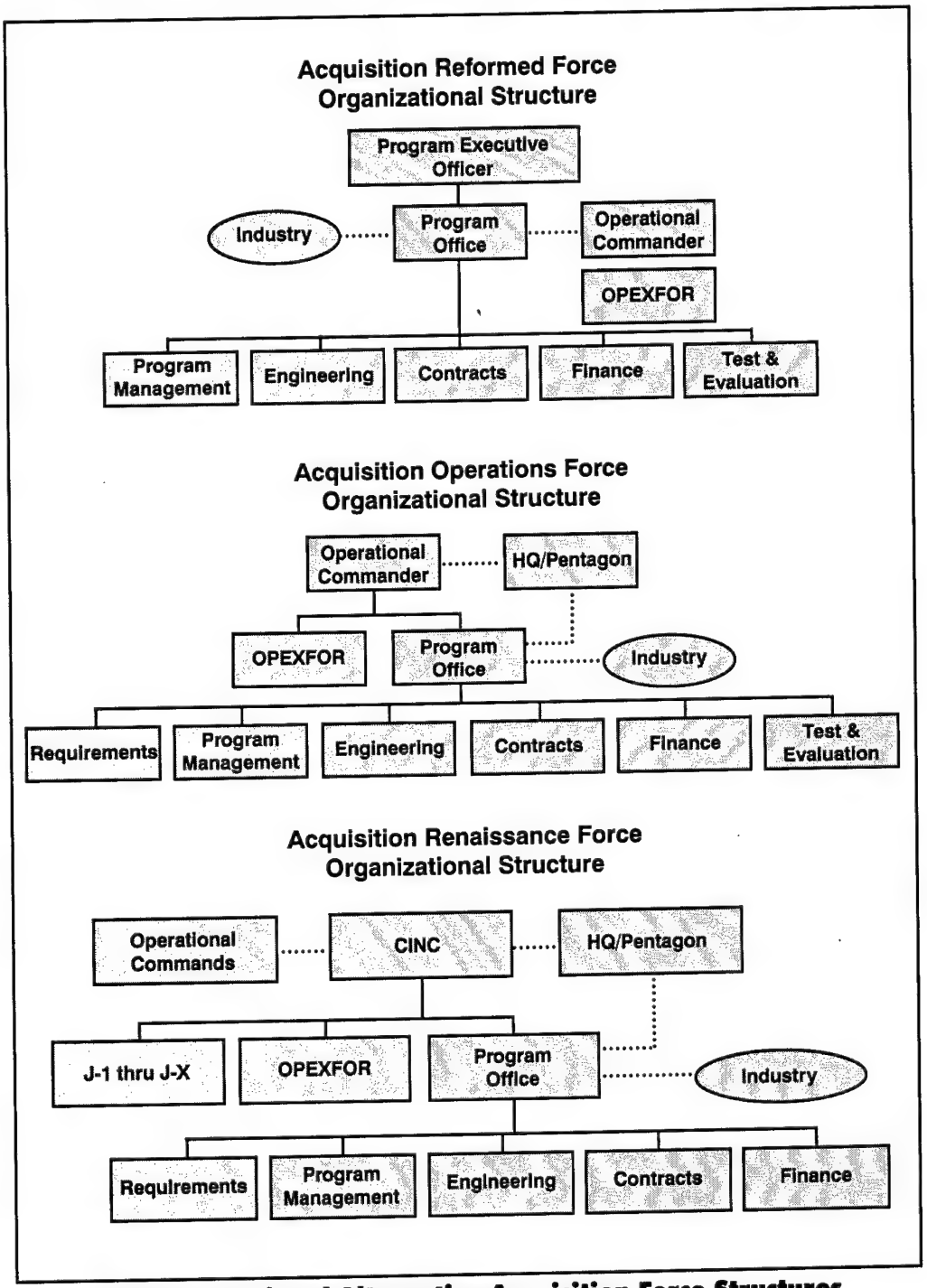


Figure 3. Notional Alternative Acquisition Force Structures

ACQUISITION REVIEW QUARTERLY
GUIDELINES FOR CONTRIBUTORS

The *Acquisition Review Quarterly (ARQ)* is a scholarly peer-reviewed journal published by the Defense Acquisition University. All submissions receive a masked review to ensure impartial evaluation.

Submissions

Submissions are welcomed from anyone involved in the Defense acquisition process. Defense acquisition is defined as the conceptualization, initiation, design, development, test, contracting, production, deployment, logistic support, modification, and disposal of weapons and other systems, supplies, or services to satisfy Defense Department needs, or intended for use in support of military missions.

Research Articles

Manuscripts should reflect research or empirically-supported experience in one or more of the aforementioned areas of acquisition. Research or tutorial articles should not exceed 4,500 words. Opinion pieces should be limited to 1,500 words.

We publish Defense Acquisition research articles that involve systemic inquiry into a significant research question. The article must produce a new or revised theory of interest to the acquisition community. You must use a reliable, valid instrument to provide your measured outcomes.

Manuscript Sections

The introduction should state the purpose of the article and concisely summarize the rationale for the undertaking.

The methods section should include a detailed methodology that clearly describes work performed. Although it is appropriate to refer to previous publications in this section, the author should provide enough information so that the experienced reader need not read earlier works to gain understanding of the methodology.

The results section should concisely summarize findings of the research and follow the train of thought established in the methods section. This section should not refer to previous publications, but should be devoted solely to the current findings of the author.

The discussion section should emphasize the major findings of the study and its significance. Information presented in the aforementioned sections should not be repeated.

Research Considerations

Contributors should also consider the following questions in reviewing their research-based articles prior to submission:

- Is the research question significant?
- Are research instruments reliable and valid?
- Are outcomes measured in a way clearly related to the variables under study?
- Does the research design fully and unambiguously test the hypothesis?
- Did you build needed controls into the study?

Contributors of research-based submissions are also reminded they should share any materials and methodology necessary to verify their conclusions.

Criteria for Tutorials

Tutorials should provide special instruction or knowledge relevant to an area of defense acquisition to inform the Defense Acquisition Workforce.

Topics for submissions should rely on or be derived from observation or experiment, rather than theory. The submission should provide knowledge in a particular area for a particular purpose.

Opinion Criteria

Opinion articles should reflect judgments based on the special knowledge of the expert. Opinion articles should be based on observable phenomena and presented in a factual manner; that is, submissions should imply detachment. The observation and judgment should not reflect the author's personal feelings or thoughts. Nevertheless, opinion pieces should clearly express a fresh point of view, rather than negatively criticize the view of another previous author.

Manuscript Style

We will require you to recast your last version of the manuscript, especially citations (e.g., footnotes or endnotes) into the format required in two specific style manuals. The *ARQ* follows the author (date) form of citation. We expect you to use the Publication Manual of the American Psychological Association (4th Edition), and the Chicago Manual of Style (14th Edition). The *ARQ* follows the author (date) form of citation.

Contributors are encouraged to seek the advice of a reference librarian in completing citations of government documents. Standard formulas of citations may give only incomplete information in reference to government works. Helpful guidance is also available in Garner, D.L. and Smith, D.H., 1993, The Complete Guide to Citing Government Documents: A Manual for Writers and Librarians (Rev. Ed.), Bethesda, MD: Congressional Information Service, Inc.

Copyright Information

The *ARQ* is a publication of the United States Government and as such is not copyrighted. Contributors of copyrighted works and copyright holders of works for hire are strongly encouraged to request that a copyright notification be placed on their published work as a safeguard against unintentional infringement. The work of federal employees undertaken as part of their official duties is not subject to copyright.

In citing the work of others, it is the contributor's responsibility to obtain permission from a copyright holder if the proposed use exceeds the fair use provisions of the law (see U.S. Government Printing Office, 1994, Circular 92: Copyright Law of the United States of America, p. 15, Washington, DC: Author). Contributors will be required to submit a copy of the written permission to the editor before publication.

Manuscript Format

Pages should be double-spaced and organized in the following order: title page, abstract, body, reference list, author's note (if any), and figures or tables. To ensure anonymity, each paper should be submitted with a separate page that includes the author(s)'s name(s) and complete address, and the paper should include the title, abstract, keywords, body, complete set of references, along with tables and figures at the end. Authors are reminded not to refer to themselves or to their own work directly in the paper. Figures or tables should not be inserted (or embedded, etc.) into the text, but segregated one to a page following the text. Articles must be printable within one issue and should not exceed 4,500 words for research or tutorials and 1,500 words for opinion pieces; articles will not be printed in parts or in a continuing series. If material is submitted on a computer diskette, each figure or table should be recorded in a separate, exportable file (i.e., a readable .eps file). For additional information on the preparation of figures or tables, see CBE Scientific Illustration Committee, 1988, Illustrating Science: Standards for Publication, Bethesda, MD: Council of Biology Editors, Inc. Please restructure briefing charts and slides to a look similar to those in previous issues of *ARQ*.

The author (or corresponding author in the case of multiple authorship) should attach to the manuscript a signed cover letter that provides the author's name, address, and telephone number (fax and Internet addresses are also appreciated). The letter should verify that the submission is an original product of the author; that it has not been published before; and that it is not under consideration by another publication. Details about the manuscript should also be included in this letter: for example, its title, word length, the need for copyright notification, the identification of copyrighted material for which permission must be obtained, a description of the computer application programs and file names used on enclosed diskettes, etc. A short biography of no more than 75 words and a photo of the author will be expected from each author. Author names and e-mail addresses are not part of the 75-word count.

The letter, one copy of the printed manuscript, and any diskettes should be

sturdily packaged and mailed to: Defense Systems Management College, Attn: DSMC Press (*ARQ*), 9820 Belvoir Road, Suite 3, Fort Belvoir, VA 22060-5565.

In most cases, the author will be notified that the submission has been received within 48 hours of its arrival. Following an initial review, submissions will be referred to referees and subsequent consideration by the *ARQ* Editorial Board.

Contributors may direct their questions to the Editor, *ARQ*, at the address shown above, by calling (703) 805-4290 (fax 805- 2917), or via the Internet at:

gonzalezd@dsmc.dsm.mil

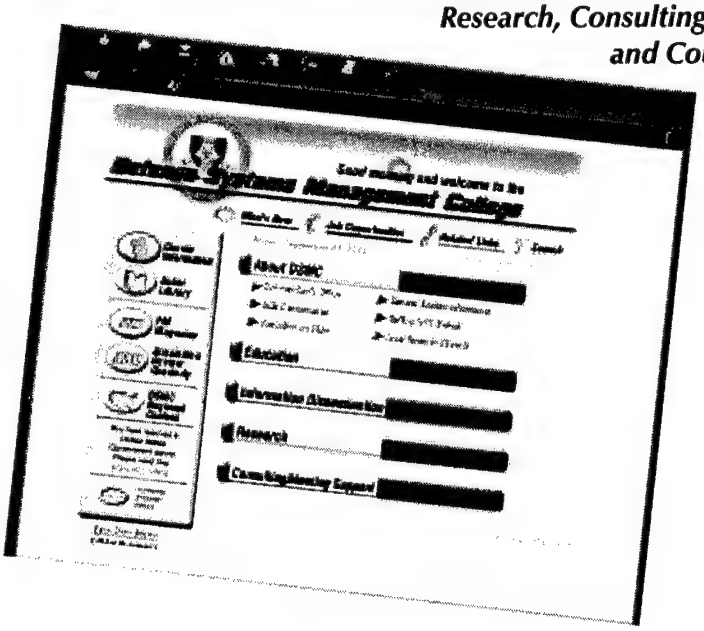
The DSMC Home Page can be accessed at:

http://www.dsmc.dsm.mil

DSMC'S Home Page

http://www.dsmc.dsm.mil

Your Online Access to Acquisition Research, Consulting, Information, and Course Offerings



Front Page

- Course Information
- David D. Acker Library
- PM Magazine
- ARQ Magazine
- What's New
- Acquistion Related Links

About DSMC

- Commandant's office
- DSMC Information
- Executive Institute
- General Student Information
- Getting to Ft. Belvoir
- Local News and Events

Education

- Acquisition Reform Learning Module
- Continuing Education
- Distance Learning
- DCAS
- DSMC Alumni Association (DSMCAA)
- DSMC Course List
- DSMC Divisions
- Education Opportunities
- EPMC
- EPMC Extranet
- Faculty Departments
- General Student Information
- IEVMC
- Individual Learning Program
- International Acquistion
- Learning Resource Center
- Past Performance
- Program Management
- Regional Centers
- Registrar

Information Dissemination

- Acquisition Events
- Best Practices
- Lessons Learned
- Links to Related Sites
- Manufacturing Resources
- Past Performance
- Publications
- Services

Research

- Acquisition Events
- Best Practices
- Lessons Learned
- DSMC Military Research Fellows
- Overview/Projects
- ROAR

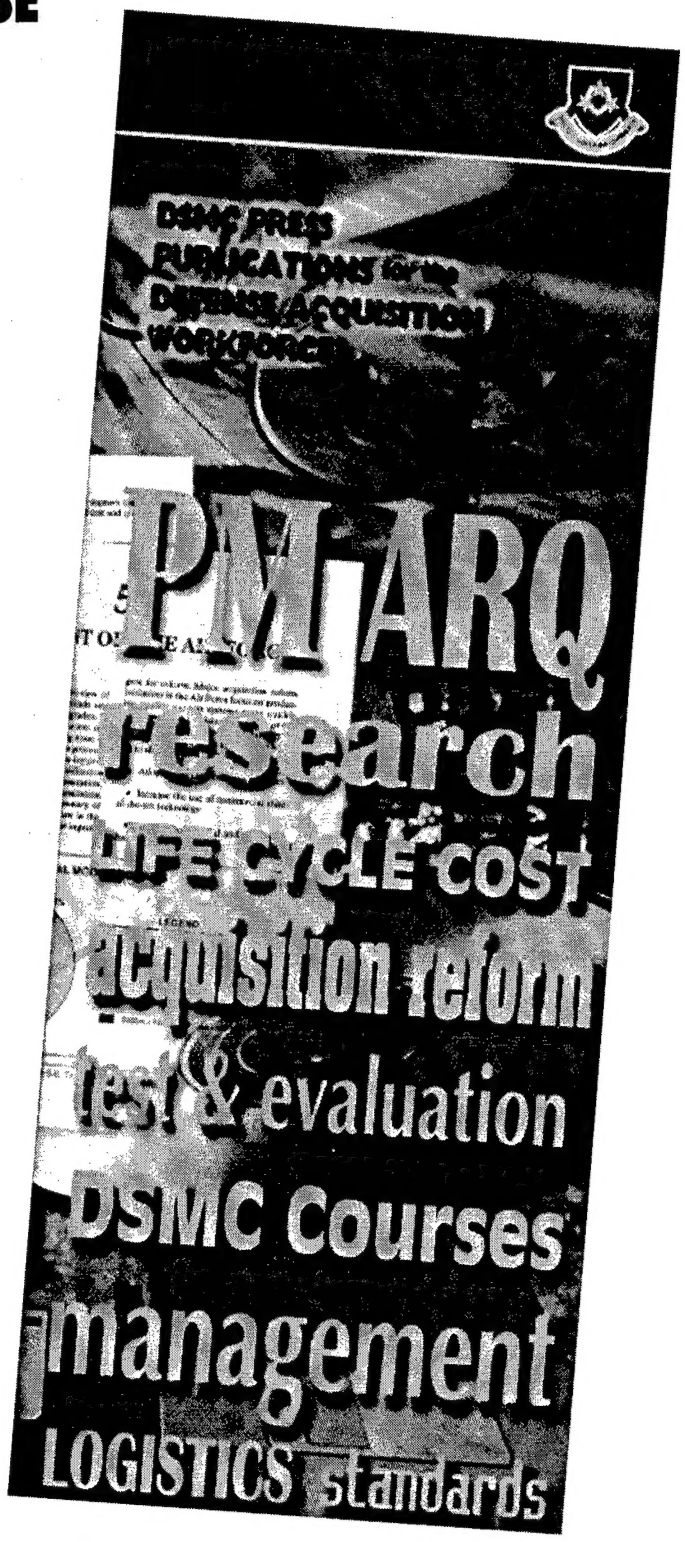
Consulting/Meeting Support

- Consulting Services
- MDC/Group Services
- Acquisition Reform Learning Model

Now you can search the DSMC Website and our on-line publications!

DSMC PRESS PUBLICATIONS FOR THE DEFENSE ACQUISITION WORKFORCE

Newly revised and updated, this free brochure is yours by faxing a request to the DSMC Press: (703) 805-2917 or DSN 655-2917. The brochure lists the publications offered by and through the College, including titles, abstracts, prices, sources, and reference numbers.



PM/ARQ SUBSCRIPTIONS

FREE SUBSCRIPTIONS

☐ ***PROGRAM MANAGER* MAGAZINE (*PM*)**
NOW FREE TO EVERYONE
☐ ***ACQUISITION REVIEW QUARTERLY (ARQ)***

NAME AND TITLE (PLEASE PRINT)

ORGANIZATION

ADDRESS

CITY STATE ZIP ( ) DAYTIME PHONE

WORK E-MAIL HOME E-MAIL

DATE SIGNED

CHANGE OF ADDRESS

☐ ***PROGRAM MANAGER* MAGAZINE (*PM*)**
☐ ***ACQUISITION REVIEW QUARTERLY (ARQ)***

NAME AND TITLE (PLEASE PRINT)

ORGANIZATION

ADDRESS

CITY STATE ZIP ( ) DAYTIME PHONE

WORK E-MAIL HOME E-MAIL

DATE SIGNED

NO POSTAGE
NECESSARY
IF MAILED
IN THE
UNITED STATES

BUSINESS REPLY MAIL
FIRST CLASS PERMIT NO. 12 FORT BELVOIR, VA

POSTAGE WILL BE PAID BY ADDRESSEE

DEPARTMENT OF DEFENSE
DEFENSE SYST MGMT COLLEGE
ATTN DSMC PRESS
9820 BELVOIR ROAD
SUITE 3
FT BELVOIR VA 22060-9989

NO POSTAGE
NECESSARY
IF MAILED
IN THE
UNITED STATES

BUSINESS REPLY MAIL
FIRST CLASS PERMIT NO. 12 FORT BELVOIR, VA

POSTAGE WILL BE PAID BY ADDRESSEE

DEPARTMENT OF DEFENSE
DEFENSE SYST MGMT COLLEGE
ATTN DSMC PRESS
9820 BELVOIR ROAD
SUITE 3
FT BELVOIR VA 22060-9989

ARQ

Acquisition Review Quarterly